

BAB IV PENGUJIAN DAN ANALISIS

Pada bab ini akan dibahas mengenai skenario pengujian yang dilakukan terhadap aplikasi yang meliputi aspek *prototype* aplikasi, performa aplikasi, dan kualitas suara yang dihasilkannya. Selanjutnya hasil pengujian akan dianalisis dari beberapa segi, untuk mengetahui kesesuaian aplikasi terhadap persyaratan standar yang telah ada sehingga mencapai tujuan yang telah ditentukan. Hasil analisis ini pada akhirnya akan digunakan untuk dijadikan bahan hipotesis guna penelitian dan pengembangan komunikasi VoIP lebih lanjut.

4.1. Pengujian *Prototype* Aplikasi

Salah satu teknik yang digunakan pada pengujian *prototype* aplikasi VoIP Steganografi adalah *Black-Box Testing* [15]. *Black-Box Testing* adalah suatu teknik pengujian yang mengamati proses masukan dan keluaran dari sistem perangkat lunak tanpa memperhatikan apa yang terjadi di dalam sistem. Salah satu cara yang terdapat pada *Black-Box Testing* adalah dengan membuat tabel-tabel yang di dalamnya berisi skenario, *output* yang diharapkan dan validasi. Hal tersebut dilakukan untuk menguji kesesuaian antara desain dengan implementasi.

Tabel 4.1. *Test Case* Identifikasi Pengguna

No.	Skenario	<i>Output</i> yang diharapkan	Validasi
1.	<i>User</i> memasukkan alamat IP yang sesuai	Aplikasi menampilkan koneksi yang terbentuk	✓
2.	<i>User</i> tidak memasukkan alamat IP	Aplikasi menampilkan pesan : Tidak dapat menentukan alamat yang dituju	✓
3.	<i>User</i> memasukkan alamat IP yang berbeda	Aplikasi menampilkan pesan : Tidak dapat terhubung ke tujuan	✓
4.	Kedua <i>user</i> saling menekan tombol tunggu	Aplikasi menampilkan pesan : Terjadi kesalahan yang tak terduga: Alamat sedang digunakan	✓
5.	Kedua <i>user</i> saling menekan tombol koneksi	Aplikasi menampilkan pesan : Terjadi kesalahan yang tak terduga: Alamat sedang digunakan	✓

*) Keterangan : ✓ = sesuai desain

Pada Tabel 4.1 memperlihatkan hasil uji *Black-Box Testing* atas identifikasi pengguna. Pengujian ini dilakukan sebelum koneksi antar dua pengguna terbentuk untuk mengetahui keberhasilan koneksi atas setiap pengujian yang dilakukan. Pada kondisi ini terdapat lima kemungkinan pengujian yang mengidentifikasi terbentuknya suatu koneksi antara dua pengguna. Hasil yang diperoleh dari pengujian menunjukkan bahwa desain yang diimplementasikan telah sesuai dengan skenario yang dirancang.

Tabel 4.2. *Test Case* Proses Komunikasi

No.	Skenario	<i>Output</i> yang diharapkan	Validasi
1.	<i>User</i> mengetikkan data teks kemudian menekan tombol 'Kirim'	Pada tampilan pengirim : Indikator Tx berwarna hijau Teks yang dikirim tertulis pada jendela Data StegoText Pada tampilan penerima : Indikator Rx berwarna hijau Teks yang diterima tertulis pada jendela Data StegoText	✓
2.	<i>User</i> tidak mengetikkan data teks kemudian menekan tombol 'Kirim'	Aplikasi menampilkan pesan : Input StegoText tidak ada. Silahkan Anda masukkan data teks yang akan dikirim ...	✓
3.	<i>User</i> menekan tombol 'Enter' setelah selesai mengetik data teks	Pada tampilan pengirim : Indikator Tx berwarna hijau Teks yang dikirim tertulis pada jendela Data StegoText Pada tampilan penerima : Indikator Rx berwarna hijau Teks yang diterima tertulis pada jendela Data StegoText	✓
4.	<i>User</i> menekan tombol 'Putus Koneksi'	Aplikasi akan tertutup/selesai	✓

*) Keterangan : ✓ = sesuai desain

Pada Tabel 4.2 memperlihatkan hasil uji *Black-Box Testing* atas proses komunikasi yang telah terbentuk.

Universitas Indonesia

Pengujian ini dilakukan setelah proses identifikasi pengguna berhasil dijalankan untuk mengetahui proses pertukaran data paket antar dua pengguna. Dari hasil pengujian yang didapatkan, bisa diketahui bahwa selama proses komunikasi antar dua pengguna, semua kemungkinan kondisi yang dipersyaratkan telah sesuai dengan desain yang dirancang.

4.2. Pengujian Performa Aplikasi

Pengujian performa aplikasi bertujuan untuk mengetahui beberapa hal yang berkaitan dengan teknik steganografi, antara lain efektifitas teknik steganografi serta pengaruhnya terhadap komunikasi VoIP maupun sebaliknya. Salah satu segi untuk mengukur efektifitas steganografi bisa diketahui dari banyaknya data yang bisa disembunyikan dan waktu yang dibutuhkan untuk proses eksekusinya. Pengujian performa waktu terhadap *prototype* aplikasi dilakukan pada proses komunikasi untuk mengetahui *delay* antar *user* VoIP Steganografi dengan beberapa ukuran data teks yang telah ditentukan.

Pengujian pengukuran waktu dilakukan setelah *user* melakukan proses pemanggilan dan terbentuk koneksi sehingga dapat memulai percakapan suara, yaitu pada saat mulai ditekan tombol 'Kirim' pada aplikasi VoIP Steganografi dan diakhiri pada saat data teks yang dikirimkan telah diterima semua oleh *user*.

Tabel 4.3. *Delay* yang dihasilkan dengan Media Telekomunikasi LAN

No.	Jumlah paket	Panjang paket rata-rata (byte)	Delay rata-rata (detik)		
			Tanpa data stego	Dengan data stego LSB 1 byte	Dengan data stego LSB 50 byte
1.	10	203,2	0,3913	1,501	1,705
2.	20	177	0,8489	2,694	2,734
3.	30	206,7	1,3261	3,516	3,756
4.	40	174,4	1,7471	4,471	4,504
5.	50	189	2,2271	5,552	5,823
6.	75	189	3,3979	7,783	8,007
7.	100	209,2	4,5565	9,963	10,423

Sedangkan untuk mengetahui pengaruh teknik steganografi pada komunikasi VoIP atau sebaliknya, dilakukan pengujian dengan menambah jumlah data yang disembunyikan pada proses *embedding*-nya.

Pengujian dilakukan pada media telekomunikasi yang berbeda, yaitu pada *Local Area Network* (LAN) dengan *bandwidth* 1 Gbps dan *Wireless Local Area Network* (WLAN) dengan *bandwidth* 54 Mbps.

Data didapatkan dengan menggunakan perangkat lunak penganalisa protokol jaringan *Wireshark 1.3.3*. Data yang diperoleh adalah rata-rata dari 10 kali hasil pengujian untuk setiap ukuran data yang dikirimkan.

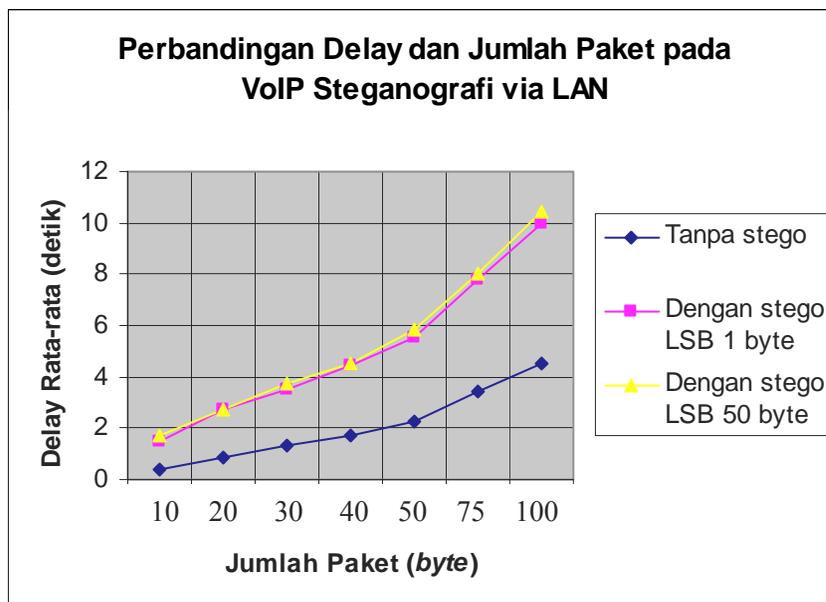
Pada Tabel 4.3 memperlihatkan hasil pengujian pengiriman data paket melalui media LAN berupa rata-rata *delay*.

Tabel 4.4. *Delay* yang dihasilkan dengan Media Telekomunikasi WLAN

No.	Jumlah paket	Panjang paket rata-rata (byte)	<i>Delay</i> rata-rata (detik)		
			Tanpa data stego	Dengan data stego LSB 1 byte	Dengan data stego LSB 50 byte
1.	10	156	0,4051	1,476	2,789
2.	20	150,2	0,8718	2,425	4,218
3.	30	160,2	1,3183	3,238	5,294
4.	40	149,4	1,7864	4,471	6,758
5.	50	158,4	2,2722	5,298	8,031
6.	75	154	3,4549	7,802	10,686
7.	100	160,9	4,5547	9,995	13,546

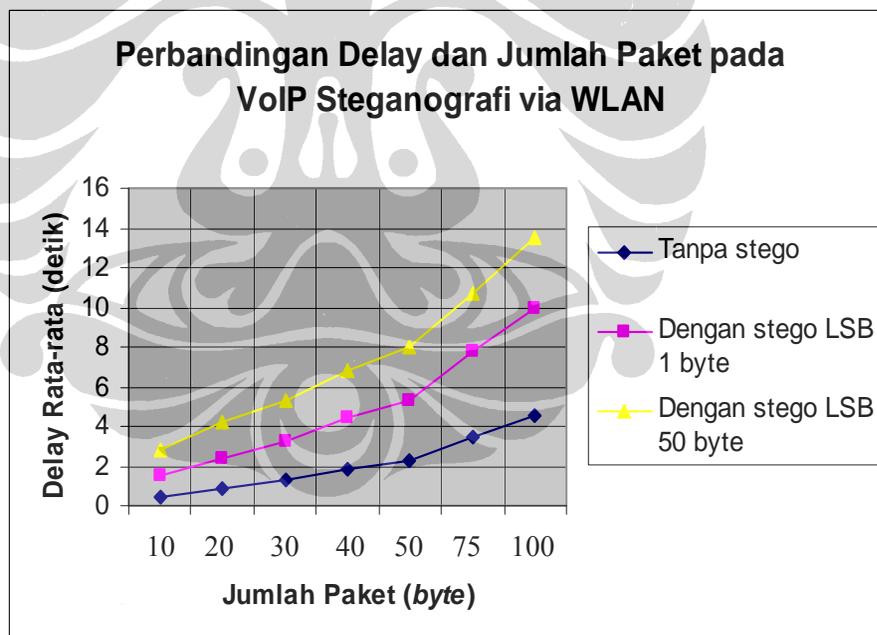
Sedangkan pada Tabel 4.4 memperlihatkan *delay* rata-rata hasil pengujian aplikasi antara dua pengguna melalui media WLAN. Hasil pengujian atas *delay* rata-rata sebagaimana terdapat pada Tabel 4.3 dan Tabel 4.4 jika digambarkan dalam bentuk grafik, akan memperlihatkan pola tertentu dengan perbedaan yang lebih jelas pada setiap pengiriman data pakatnya. Gambar 4.1 adalah representasi grafik dari Tabel 4.3, yaitu perbandingan *delay* rata-rata dan jumlah paket pada pengujian aplikasi melalui media LAN.

Universitas Indonesia



Gambar 4.1. Grafik Performa VoIP Steganografi melalui LAN

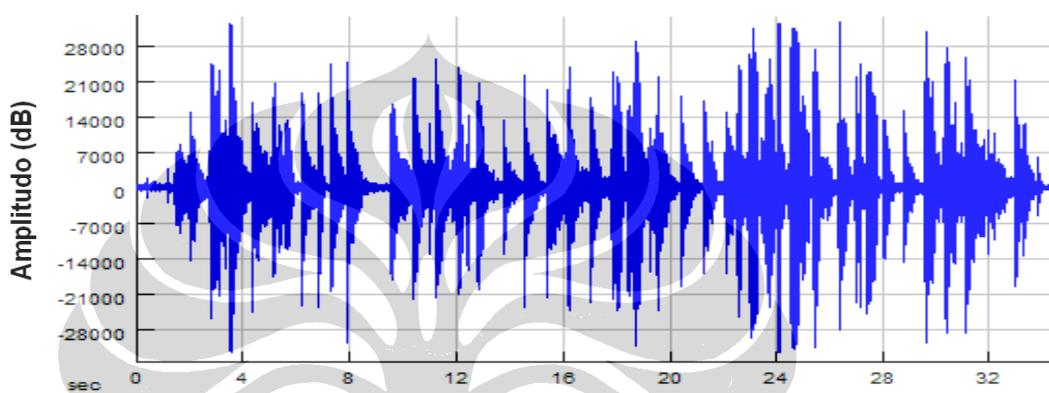
Sedangkan pada Gambar 4.2 menunjukkan grafik representasi Tabel 4.4 yaitu perbandingan *delay* rata-rata pada setiap pengiriman jumlah paket atas pengujian aplikasi melalui media WLAN.



Gambar 4.2. Grafik Performa VoIP Steganografi melalui WLAN

4.3. Pengujian Kualitas Suara

Untuk mendapatkan suara yang dihasilkan dari pengujian digunakan perangkat lunak perekam *audio streaming SoundTap v 2.01*. Suara yang dihasilkan dari proses pengujian direkam dalam file dengan format *wav*. Pengujian kualitas suara dilakukan dengan menggunakan perangkat lunak pengolah suara *Sigview 2.2.0* untuk mengetahui pola *waveform* yang dihasilkan. Dari pola *waveform* yang terbentuk akan dianalisis untuk mengetahui indikasi adanya steganografi pada VoIP. Disamping itu, pengujian kualitas suara juga dilakukan dengan menggunakan perangkat lunak pemroses audio dan percakapan *SP Demo 3.0* dari Technion IIT. File *wav* hasil rekaman akan digunakan untuk mengetahui nilai *Signal to Noise Ratio (SNR)* dan nilai *Perceptual Evaluation of Speech Quality (PESQ)* [3].



Gambar 4.3. Pola *Waveform* VoIP tanpa Data Stego melalui LAN

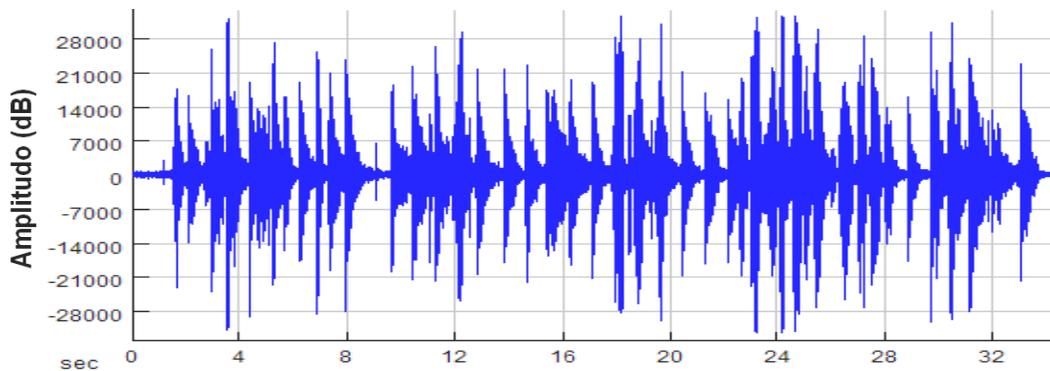
Kualitas suara yang didapatkan dari hasil pengujian akan digunakan untuk mengetahui kesesuaian aplikasi terhadap standar komunikasi VoIP yang telah ditentukan. Selain itu, kualitas suara yang dihasilkan akan dianalisis terhadap pemenuhan kriteria steganografi untuk mengetahui bahwa teknik steganografi yang digunakan bisa menjamin keamanan datanya sesuai dengan yang diharapkan.

Untuk memperoleh perbandingan yang setara atas hasil kualitas suara yang direkam, diperlukan sumber suara yang sama. Dalam pengujian ini sumber suara yang digunakan adalah 30 detik pertama lagu Akal Sehat dari Ada Band. Suara yang terdengar pada pihak penerima akan direkam dalam file dengan format *wav*.

Hasil rekaman direpresentasikan dalam bentuk grafik amplitudo untuk setiap jenis pengujian.

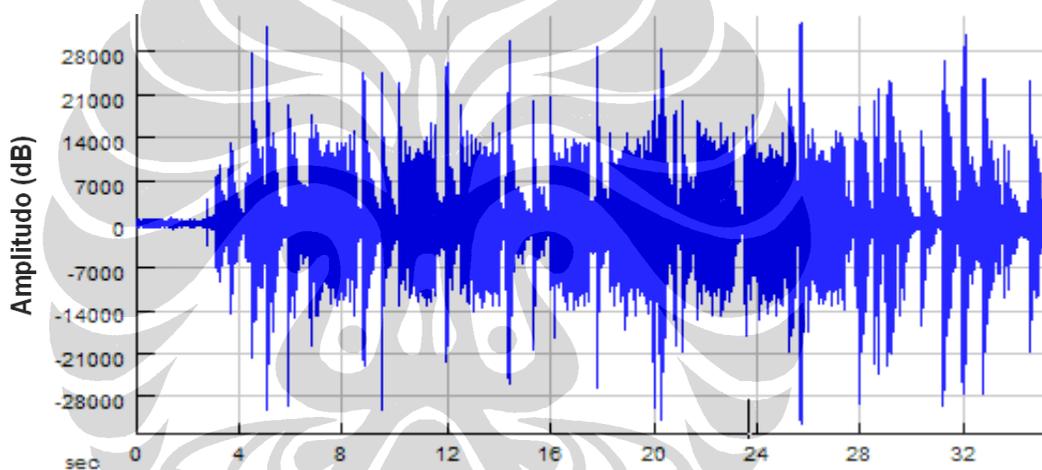
Universitas Indonesia

Pada Gambar 4.3 memperlihatkan pola *waveform* VoIP tanpa data stego melalui LAN. Jika dibandingkan pola yang terbentuk dengan pola pada Gambar 4.4 terdapat sedikit perbedaan.



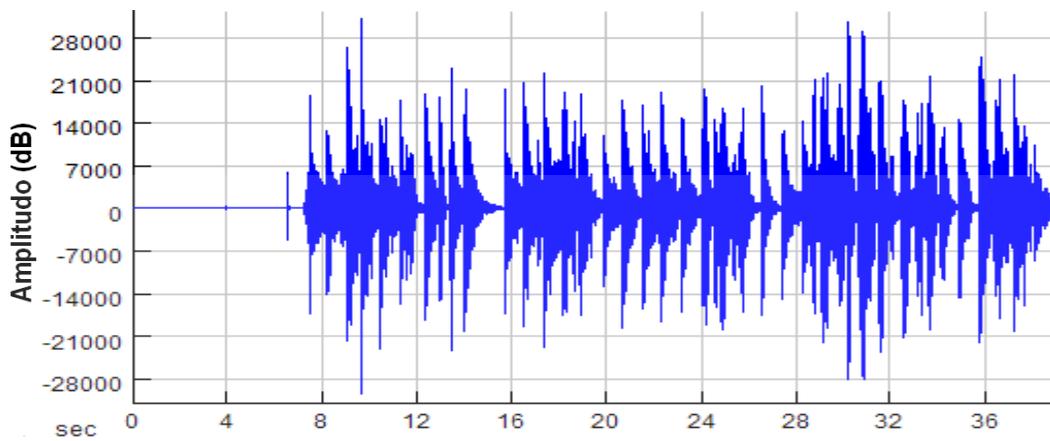
Gambar 4.4. Pola *Waveform* VoIP dengan Data Stego LSB 1 *byte* melalui LAN

Grafik amplitudo pada Gambar 4.4 menunjukkan pola *waveform* VoIP yang dihasilkan atas rekaman suara yang telah ditempel data dengan stego 1 *byte*.



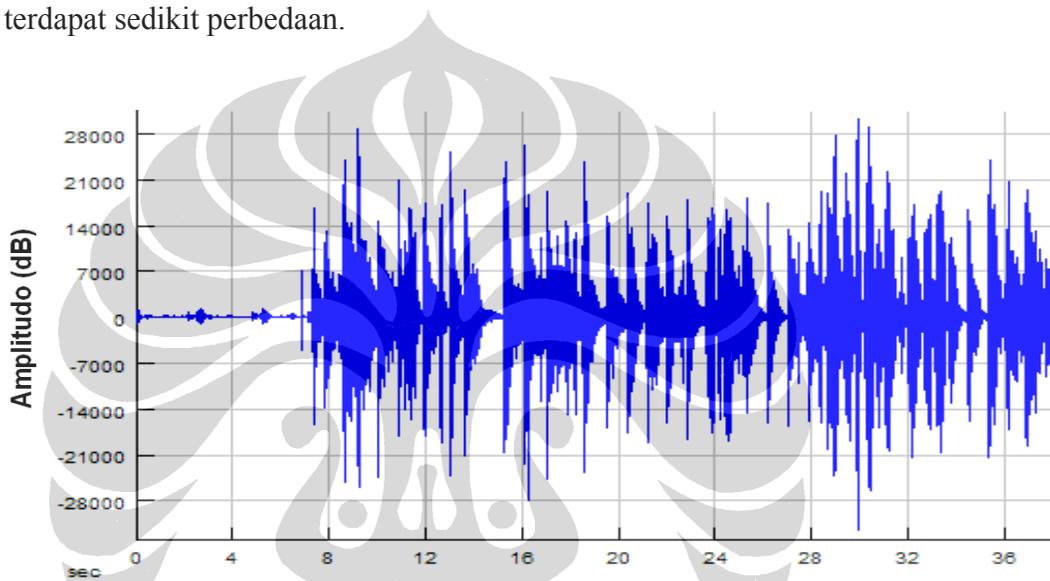
Gambar 4.5. Pola *Waveform* VoIP dengan Data Stego LSB 50 *byte* melalui LAN

Sedangkan pada Gambar 4.5 menunjukkan pola *waveform* VoIP yang dihasilkan dari rekaman suara yang telah ditempel dengan data stego 50 *byte*. Pada pola *waveform* ini jika diperhatikan dengan seksama akan lebih memperlihatkan perbedaan yang sangat mencolok dibandingkan pola *waveform* rekaman suara aslinya. Terdapatnya pola-pola tertentu dengan bentuk-bentuk yang mirip dan berulang-ulang akan menjadi bahan analisis atas kualitas suara yang dihasilkan.



Gambar 4.6. Pola *Waveform* VoIP tanpa Data Stego melalui WLAN

Pada Gambar 4.6 memperlihatkan pola *waveform* VoIP tanpa data stego melalui WLAN. Jika dibandingkan pola yang terbentuk dengan pola pada Gambar 4.7 juga terdapat sedikit perbedaan.

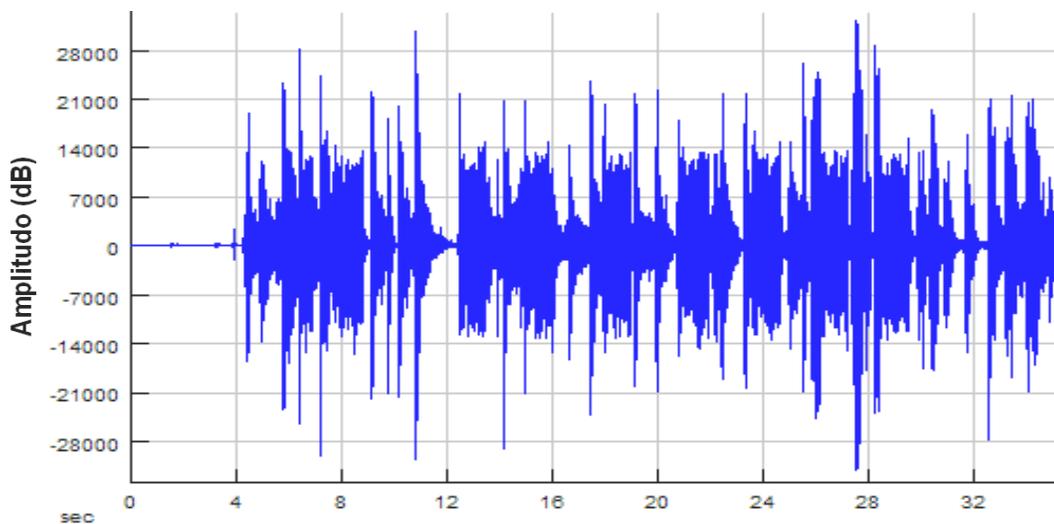


Gambar 4.7. Pola *Waveform* VoIP dengan Data Stego LSB 1 *byte* melalui WLAN

Grafik amplitudo pada Gambar 4.7 menunjukkan pola *waveform* VoIP Steganografi pada media WLAN yang dihasilkan atas rekaman suara yang telah ditempel data dengan stego 1 *byte*.

Sedangkan pada Gambar 4.8 menunjukkan pola *waveform* VoIP Steganografi pada media WLAN yang dihasilkan dari rekaman suara yang telah ditempel dengan data stego 50 *byte*. Pada pola *waveform* ini jika diperhatikan dengan seksama akan lebih memperlihatkan perbedaan yang sangat mencolok dibandingkan pola *waveform*

rekaman suara aslinya. Pada grafik amplitudonya juga terdapat pola-pola tertentu dengan bentuk-bentuk yang mirip dan berulang-ulang.



Gambar 4.8. Pola *Waveform* VoIP dengan Data Stego LSB 50 *byte* melalui WLAN

Hasil pengukuran nilai SNR dan PESQ atas kualitas suara yang telah direkam dapat dilihat pada Tabel 4.5 berikut.

Tabel 4.5. Hasil Pengukuran Nilai SNR dan PESQ

No.	Jenis Rekaman Suara	SNR (dB)		PESQ	
		Via LAN	Via WLAN	Via LAN	Via WLAN
1.	Tanpa stego	30,4359	21,3698	4,5	4,5
2.	Dengan stego 1 <i>byte</i>	31,0458	21,0262	4,5	4,5
3.	Dengan stego 50 <i>byte</i>	18,3037	18,0807	4,5	4,5

4.4. Analisis

Dari hasil pengujian terhadap aplikasi VoIP Steganografi telah diperoleh ukuran-ukuran yang dapat digunakan untuk mengetahui keberhasilan aplikasi, efektifitas teknik steganografi, pengaruh teknik steganografi pada komunikasi VoIP, serta tingkat keamanan data yang dikirimkan.

Universitas Indonesia

4.4.1. Analisis Hasil Pengujian Performa Aplikasi

Hasil yang diperoleh pada pengukuran *delay* baik yang dilakukan pada media telekomunikasi LAN maupun WLAN dengan pengiriman ukuran paket yang berbeda-beda seperti yang terlihat pada Tabel 4.3 dan Tabel 4.4 menunjukkan bahwa terdapat peningkatan waktu *delay* yang cenderung linear terhadap ukuran paket yang dikirimkan. Kecenderungan ini membentuk *trend* grafik yang bila diformulasikan akan menghasilkan persamaan sebagai berikut :

$$y = 1,3845x - 0,2593 \dots\dots\dots (4.1)$$

Formula persamaan ini bisa diketahui secara otomatis melalui penggambaran grafik dengan menggunakan *Microsoft Excel 2007*.

Pengukuran *delay* dengan paket tanpa data stego menunjukkan kinerja aplikasi VoIP sesungguhnya, sedangkan setelah diujicoba dengan mengirimkan data menggunakan metode steganografi LSB 1 *byte* atau LSB 50 *byte* terdapat peningkatan waktu *delay* dibandingkan *delay* kinerja sesungguhnya. Metode LSB 1 *byte* artinya bahwa data yang ditempelkan/disembunyikan pada paket suara adalah sebesar 1 *byte* untuk setiap paketnya. Peningkatan waktu *delay* setelah pengiriman data disebabkan oleh proses *embedding* data sebelum data dikirimkan dan proses ekstraksinya pada saat penerimaan paket datanya. Semakin besar/banyak data yang dikirimkan semakin besar pula waktu yang diperlukan untuk proses *embedding* dan ekstraksinya.

Tabel 4.6. Prosentase Peningkatan *Delay* dengan Media Telekomunikasi LAN

No.	Jumlah paket	<i>Delay</i> (detik)			Prosentase peningkatan <i>delay</i> (%)	
		Tanpa data stego	Dengan data stego LSB 1 <i>byte</i>	Dengan data stego LSB 50 <i>byte</i>	Dengan data stego LSB 1 <i>byte</i>	Dengan data stego LSB 50 <i>byte</i>
1.	10	0,3913	1,501	1,705	292,2821	303,5267
2.	20	0,8489	2,694	2,734	162,3395	193,9098
3.	30	1,3261	3,516	3,756	145,3812	165,5154
4.	40	1,7471	4,471	4,504	157,9704	171,3067
5.	50	2,2271	5,552	5,823	149,2479	158,2282
6.	75	3,3979	7,783	8,007	126,5223	135,2041
7.	100	4,5565	9,963	10,423	124,2291	128,2015
Rata-rata prosentase peningkatan <i>delay</i> :					165,4246	179,4132

Pada pengukuran *delay* dengan media telekomunikasi LAN dapat diketahui bahwa terdapat peningkatan *delay* untuk setiap peningkatan jumlah paket. Pada pengiriman data sebesar 10 paket terdapat peningkatan sebesar $1,501 - 0,3913 = 1,1097$ detik atau 292,3%. Prosentase peningkatan waktu *delay* untuk pengiriman data selanjutnya dapat dilihat pada Tabel 4.6.

Tabel 4.7. Prosentase Peningkatan *Delay* dengan Media Telekomunikasi WLAN

No.	Jumlah paket	<i>Delay</i> (detik)			Prosentase peningkatan <i>delay</i> (%)	
		Tanpa data stego	Dengan data stego LSB 1 <i>byte</i>	Dengan data stego LSB 50 <i>byte</i>	Dengan data stego LSB 1 <i>byte</i>	Dengan data stego LSB 50 <i>byte</i>
1.	10	0,4051	1,476	2,789	280,4124	618,8144
2.	20	0,8718	2,425	4,218	207,663	435,1434
3.	30	1,3183	3,238	5,294	160,7715	326,351
4.	40	1,7864	4,471	6,758	169,5972	307,5012
5.	50	2,2722	5,298	8,031	146,7055	273,9697
6.	75	3,4549	7,802	10,686	143,7135	233,8019
7.	100	4,5547	9,995	13,546	145,3062	232,458
Rata-rata prosentase peningkatan <i>delay</i> :					179,167	346,8628

Pada Tabel 4.6 dan 4.7 terlihat bahwa prosentase peningkatan *delay* pada media telekomunikasi WLAN lebih besar dibandingkan dengan prosentase peningkatan *delay* pada media telekomunikasi LAN. Hal ini bisa disebabkan oleh perbedaan *bandwidth* yang digunakan pada masing-masing media telekomunikasi.

Jika diambil pembulatan satu desimal, pada Tabel 4.6 dapat terlihat bahwa untuk pengiriman data sebesar 100 paket pada media telekomunikasi LAN dengan data stego 1 *byte* diperlukan waktu sekitar 10 detik, sedangkan dengan data stego 50 *byte* diperlukan waktu sekitar 10,4 detik. Sedangkan untuk pengiriman data pada media telekomunikasi WLAN untuk data sebesar 100 paket (Tabel 4.7) hanya terdapat perbedaan pada pengiriman paket dengan data stego 50 *byte*, yaitu memerlukan waktu sekitar 13,5 detik. Jadi untuk mengirimkan data teks sebanyak satu paragraf yang terdiri dari sekitar 100 kata (lebih kurang 750 karakter) dan dikirimkan baik melalui media telekomunikasi LAN maupun WLAN dengan data stego 1 *byte*

diperlukan waktu sekitar $0,1 \times 750 = 75$ detik (1 menit 15 detik). Sedangkan jika menggunakan data stego 50 *byte* pada media telekomunikasi LAN memerlukan waktu sekitar $0,104 \times 750 = 78$ detik (1 menit 18 detik) dan pada media telekomunikasi WLAN memerlukan waktu sekitar $0,135 \times 750 = 101,25$ detik (1 menit 41,25 detik). Selisih waktu yang diperlukan untuk pengiriman data sebesar 1 paragraf (sekitar 750 karakter) dengan data stego 50 *byte* antara media telekomunikasi LAN dengan WLAN sebesar 23,25 detik. Waktu tersebut adalah waktu yang diperlukan dalam proses pengiriman datanya jadi tidak termasuk waktu pengetikan data teksnya. Dari hal tersebut dapat diketahui bahwa aplikasi VoIP Steganografi dengan LSB 50 *byte* lebih efektif jika digunakan pada media telekomunikasi dengan *bandwidth* yang tinggi, sedangkan untuk aplikasi VoIP Steganografi dengan LSB 1 *byte* tidak begitu terpengaruh oleh *bandwidth* yang digunakan.

Delay standar komunikasi VoIP yang ditentukan menurut rancangan Peraturan Menteri Komunikasi dan Informatika tentang Standar Wajib Kualitas Pelayanan Jasa Internet Teleponi untuk Keperluan Publik (ITKP) [13] dengan menggunakan Transmisi *Toll Quality* (Fiber Optik) adalah ≤ 50 ms (*mill seconds*), sedangkan nilai *Packet Delay* dengan menggunakan Transmisi *Below Toll Quality* (satelit) adalah ≤ 300 ms (*mill seconds*). ITU-T merekomendasikan besarnya *delay* maksimum untuk aplikasi suara adalah 150 ms [14].

Pengiriman 1 paket data pada aplikasi VoIP Steganografi dengan LSB 1 *byte* memerlukan waktu sekitar 0,09 detik (90 ms). Sehingga aplikasi ini masih memenuhi standar yang telah ditentukan, jika dibandingkan dengan standar ITU-T, sedangkan menurut standar rancangan Peraturan Menteri Komunikasi dan Informatika, nilai ini masih memenuhi syarat jika digunakan melalui transmisi satelit.

Dari Gambar 4.1 dan 4.2 dapat dilihat bahwa semakin besar/banyak data yang dikirimkan semakin besar pula *delay*-nya. Dengan membandingkan grafik peningkatan *delay* pada VoIP tanpa data stego dan VoIP dengan data stego dapat diketahui bahwa peningkatan *delay* pada VoIP dengan data stego terlihat semakin tinggi seiring dengan besarnya paket yang dikirimkan. Hal ini dapat dijadikan sebagai salah satu indikasi adanya proses steganografi pada komunikasi VoIP.

4.4.2. Analisis Hasil Pengujian Kualitas Suara

Pola *waveform* yang diperoleh dari hasil pengujian kualitas suara membentuk grafik amplitudo tertentu untuk setiap metode steganografi yang digunakan. Pada Gambar 4.3, 4.4, dan 4.5 jika diteliti dengan seksama terlihat ada perbedaan meskipun sedikit antara pola *waveform* aplikasi VoIP tanpa data stego dengan pola *waveform* aplikasi VoIP dengan data stego LSB 1 *byte*, sedangkan jika dibandingkan dengan aplikasi VoIP dengan data stego LSB 50 *byte* terdapat perbedaan yang sangat mencolok.

Pada aplikasi VoIP melalui media komunikasi WLAN (Gambar 4.6, 4.7, dan 4.8), perbedaan yang mencolok juga terlihat antara pola *waveform* tanpa data stego dan pola *waveform* dengan data stego LSB 50 *byte*. Dengan kata lain aplikasi VoIP Steganografi dengan LSB 1 *byte* ditinjau dari segi keamanan dan efektifitasnya [1] lebih baik sesuai dengan kriteria yang ada [10] dibandingkan dengan aplikasi VoIP Steganografi dengan LSB 50 *byte*.

Pada Gambar 4.5 dan 4.8 terdapat pola *waveform* yang berbeda, dimana dalam rentang grafik amplitudonya terdapat blok-blok *waveform* yang terlihat rapat dan rata serta berulang-ulang. Hal ini disebabkan oleh adanya penempelan data pada paket suara yang dikirim akibat proses steganografi. Dari pola *waveform* yang terbentuk tersebut indikasi adanya proses steganografi menjadi lebih terlihat dengan jelas. Sehingga untuk mendeteksi adanya steganografi pada komunikasi VoIP selain dengan membandingkan *delay*, juga terlihat dari pola *waveform* yang terbentuk tanpa mengesampingkan hambatan/kendala yang mempengaruhi kualitas layanan komunikasi VoIP pada umumnya, seperti *delay*, *jitter*, besarnya *bandwidth* dan sebagainya.

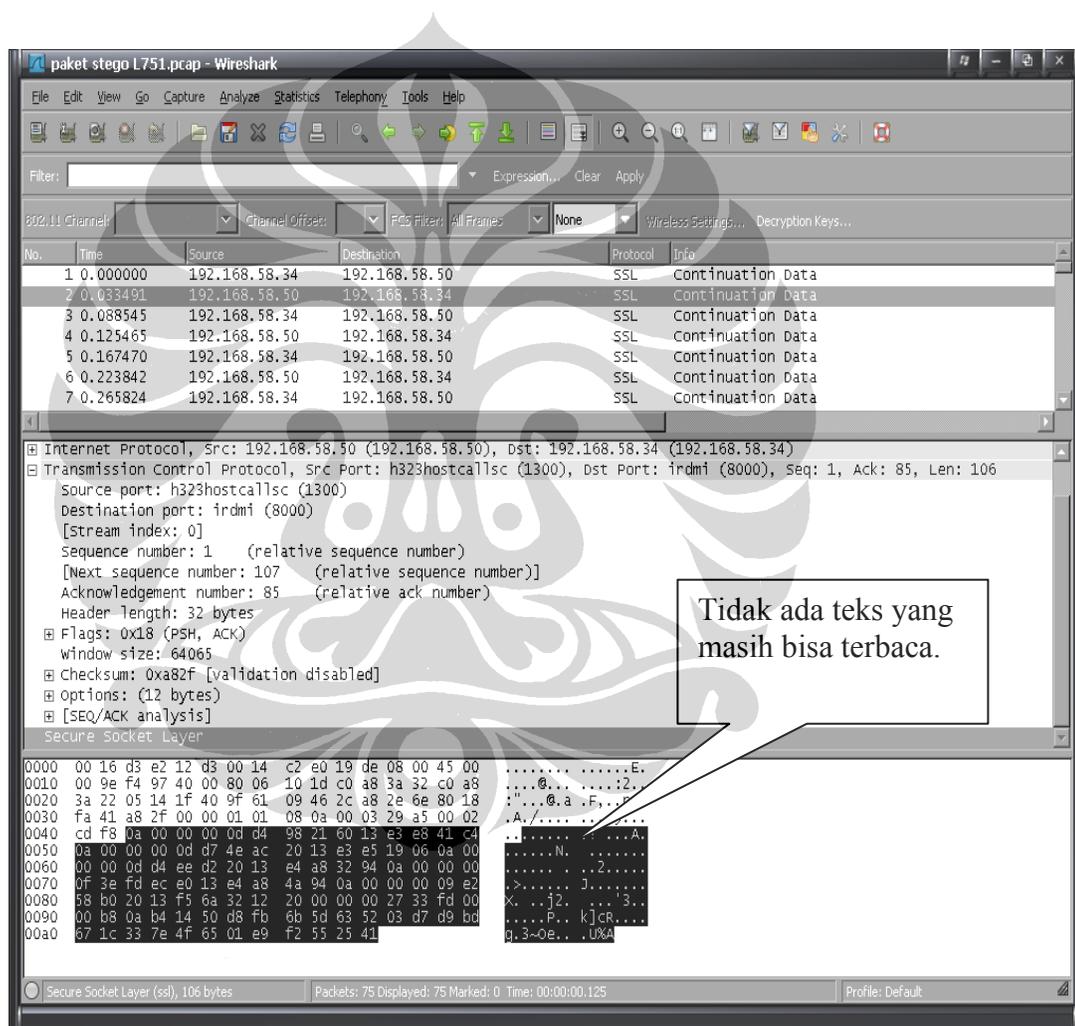
Hasil pengukuran nilai SNR dan PESQ atas pengujian kualitas suara (Tabel 4.5) dengan perangkat lunak Sigview 2.2.0 dan SP Demo 3.0 menunjukkan bahwa nilai-nilai yang diperoleh masih memenuhi standar persyaratan komunikasi VoIP secara umum.

Nilai standar minimum SNR untuk komunikasi VoIP sebagaimana yang digunakan oleh Cisco [18] adalah 25 dB, sedangkan rekomendasi minimum SNR untuk *wireless* VoIP adalah 19 dB dengan konektivitas 1 Mbps. Meskipun demikian terlihat jelas bahwa nilai SNR pada media telekomunikasi WLAN (21 dB) jauh lebih rendah

dibandingkan pada media telekomunikasi LAN (31 dB). Hal ini membuktikan bahwa media komunikasi yang digunakan pada aplikasi VoIP Steganografi sangat berpengaruh terhadap kualitas suara yang dihasilkan.

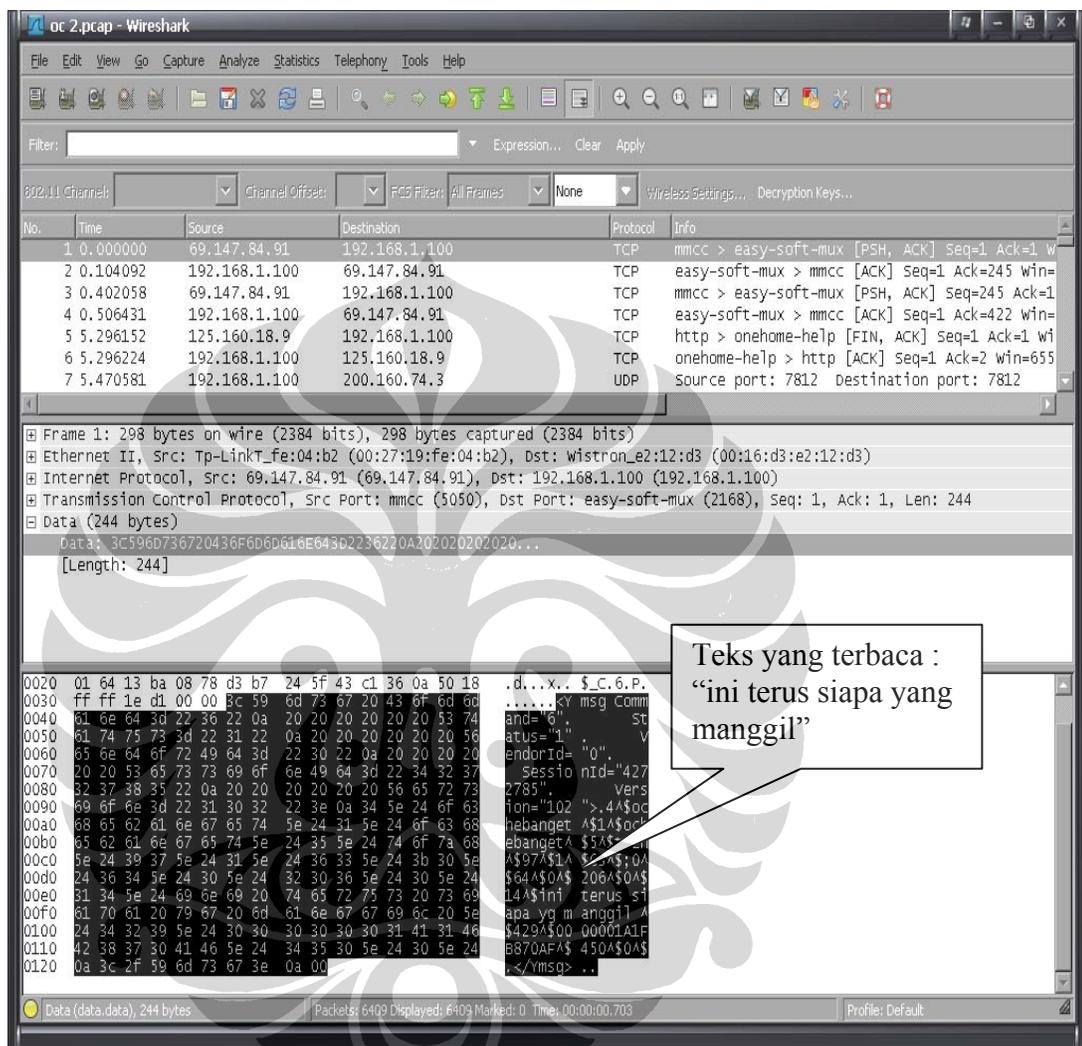
Untuk nilai PESQ [19] yang digunakan dinyatakan dalam skala -0,5 untuk yang terendah sampai dengan 4,5 untuk yang tertinggi.

Selain hal-hal yang telah disebutkan di atas, untuk membuktikan bahwa aplikasi steganografi melalui VoIP dengan masukan data teks memberikan hasil yang berbeda dengan aplikasi *instant messaging/chatting* biasa, telah dilakukan *capture*/penangkapan data yang dikirim antar aplikasi VoIP Steganografi dan data yang dikirim antar aplikasi *instant messaging*. Aplikasi *instant messaging* yang diujicoba pada pengujian ini adalah *Yahoo Messenger*. Penangkapan paket data yang dikirimkan antar aplikasi menggunakan perangkat lunak *Wireshark 1.3.3*.



Gambar 4.9. Tampilan *Capture* Paket Data Aplikasi VoIP Steganografi

Hasil penangkapan paket data antar aplikasi VoIP Steganografi menunjukkan bahwa pada data yang ditangkap tidak terdapat karakter yang masih terbaca seperti pada masukan data teksnya, karena isi data paket adalah hasil kompresi dari *voice codec* yang digunakan. Sedangkan pada aplikasi *Yahoo Messenger*, setelah data paket yang dikirim ditangkap dan dianalisa, masih terlihat adanya blok-blok karakter yang dapat dibaca sesuai dengan teks yang ditulis pada masing-masing pengguna.



Gambar 4.10. Tampilan *Capture* Paket Data Aplikasi *Yahoo Messenger*

Pada Gambar 4.9 dan 4.10 dapat dilihat hasil *capture* paket data dengan perangkat lunak *Wireshark 1.3.3* yang menunjukkan perbedaan isi paket data antara aplikasi VoIP Steganografi dengan aplikasi *Yahoo Messenger*.

Dengan demikian pengiriman data menggunakan aplikasi VoIP Steganografi lebih aman dibandingkan dengan menggunakan aplikasi *instant messaging* biasa, dalam hal ini *Yahoo Messenger*.

4.5. Kelebihan dan Kekurangan Aplikasi

Kelebihan aplikasi VoIP Steganografi adalah :

- 1) Komunikasi data teks menggunakan aplikasi VoIP Steganografi lebih aman dibandingkan dengan aplikasi *instant messaging* biasa, misalnya *Yahoo Messenger*.
- 2) Kombinasi penggunaan protokol *peer to peer* khusus dengan *voice codec* Speex pada aplikasi VoIP Steganografi lebih mempersulit analisis protokol komunikasi suara.
- 3) Proses steganografi dengan LSB 1 *byte* tidak mempengaruhi aplikasi VoIP yang digunakan, khususnya kualitas suara yang dihasilkan.

Kekurangan aplikasi VoIP Steganografi adalah :

- 1) Pengujian implementasi aplikasi VoIP Steganografi masih terbatas pada komputer dengan sistem operasi Windows XP.
- 2) Mode komunikasi suara pada aplikasi VoIP Steganografi masih *point-to-point*, belum menerapkan komunikasi suara dengan sistem konferensi.

