STUDI MENGENAI PENERAPAN STEGANOGRAFI PADA *VOIP* DENGAN LSB DAN *COVERT CHANNEL*

Diana Rosida – NIM : 13502050

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if12050@students.if.itb.ac.id

Abstrak

Steganografi merupakan salah satu teknik enkripsi yang dianggap paling aman saat ini. Steganografi menyembunyikan pesan di dalam pesan lain yang bisa berupa teks, gambar, dan sebagainya. Karena biasanya manusia kurang peka dengan pesan yang tidak berbentuk teks yang mudah terlihat, steganografi menjadi jarang terdeteksi.

Steganografi digital menggunakan beragam media digital untuk menyembunyikan pesan. Media tersebut bisa berupa gambar, audio, atau video. Teknik penyembunyian pesan yang digunakan juga beragam.

Saat ini telah banyak pendekatan untuk mendeteksi steganografi pada gambar digital. Namun, masih sedikit metode yang dipublikasi untuk mendeteksi steganografi pada data suara, padahal teknologi pengiriman data suara telah banyak yang dilengkapi dengan *field* untuk steganografi, salah satunya VoIP.

Makalah ini membahas penerapan steganografi pada VoIP. VoIP (*Voice over Internet Protocol*) merupakan salah satu media untuk berkirim pesan berbentuk suara. VoIP mengirimkan data berupa suara menggunakan paket-paket IP. Apabila suara yang berupa paket-paket IP tersebut 'dicuri' di tengah jalan, pencurinya akan segera mengetahui isinya. Untuk mengatasi hal tersebut, 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.

Dengan makalah ini, penulis ingin berbagi pengetahuan mengenai penerapan steganografi pada VoIP. Penulis berharap agar dengan makalah ini pembaca bisa terinspirasi untuk mengembangkan steganografi beserta aplikasinya khususnya pada media audio atau suara.

Kata kunci: steganografi, *Voice over Internet Protocol*, *covert channel, least significant bits*.

1. Pendahuluan

Teknologi yang semakin canggih telah memberi banyak kemudahan bagi manusia. Salah satunya adalah pertukaran pesan melalui media elektronik. Dengan menggunakan media elektronik dan jaringan komunikasi, pesan bisa dipertukarkan dengan cepat dan mudah tanpa dibatasi jarak dan waktu.

Tetapi ternyata teknologi tidak menjamin kegiatan manusia bisa bebas dari risiko. Kemudahan pertukaran pesan melalui media elektronik masih mempunyai beberapa risiko, di antaranya risiko penyadapan, pengubahan, dan perusakan pesan, sehingga diperlukan suatu cara yang bisa mengurangi dampak negatif atas terjadinya risiko tesebut. Lebih baik lagi jika cara tersebut bisa mengurangi kemungkinan terjadinya risiko yang dimaksud.

Karena alasan tersebut, muncullah penyandian terhadap pesan dengan enkripsi dan dekripsi. Enkripsi (*enciphering, standard nama menurut ISO 7498-2)* dilakukan pada pesan yang akan dikirim dengan cara mengubah pesan asli ke dalam bentuk lain yang sulit untuk dimengerti. Sedangkan dekripsi (*deciphering, standard nama menurut ISO 7498-2)* dilakukan pada pesan hasil enkripsi yang diterima dengan cara mengubahnya

kembali ke bentuk aslinya dengan kunci yang memang telah diketahui sebelumnya.

Dengan teknik tersebut, pesan yang dikirmkan selalu dalam bentuk yang sulit dimengerti sehingga yang mengetahui maksudnya hanyalah pengirimnya dan penerima yang dituju. Ilmu dan seni untuk menjaga kerahasian pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya disebut kriptografi.

Semula penyandian sederhana telah efektif untuk menjaga kerahasiaan pesan, tetapi lalu muncul kriptanalisis. Kriptanalisis adalah ilmu dan seni untuk memecahkan pesan terenkripsi menjadi bentuk aslinya tanpa mengetahui kunci yang diberikan. Karena itu kriptografi berkembang sehingga ia tidak lagi sebatas mengenkripsi pesan, tetapi juga memberikan aspek keamanan yang lain.

Bentuk pesan yang telah dienkripsi biasanya tidak lazim. Seorang penyadap yang mendapatkannya bisa langsung mengenalinya sebagai pesan terenkripsi. Karena telah dikenali oleh penyadap, risiko diketahui, diubah, dan dirusaknya pesan asli menjadi lebih besar.

Menyadari hal tersebut, para ahli kriptografi mencoba mencari cara baru yang lebih efektif. Salah satu cara yang ditemukan adalah dengan melakukan penyembunyian pesan ke dalam pesan lain sehingga pesan tersebut tidak disadari keberadaannya. Cara ini disebut steganografi.

Steganografi banyak digunakan untuk memberikan tanda (seperti *copyright*) pada suatu karya cipta yang menandakan bahwa karya cipta tersebut bukan bajakan. Selain itu steganografi juga seringkali digunakan untuk menyembunyikan pesan rahasia yang ditujukan kepada orang tertentu.

2. Steganografi

2.1. Pengertian Steganografi

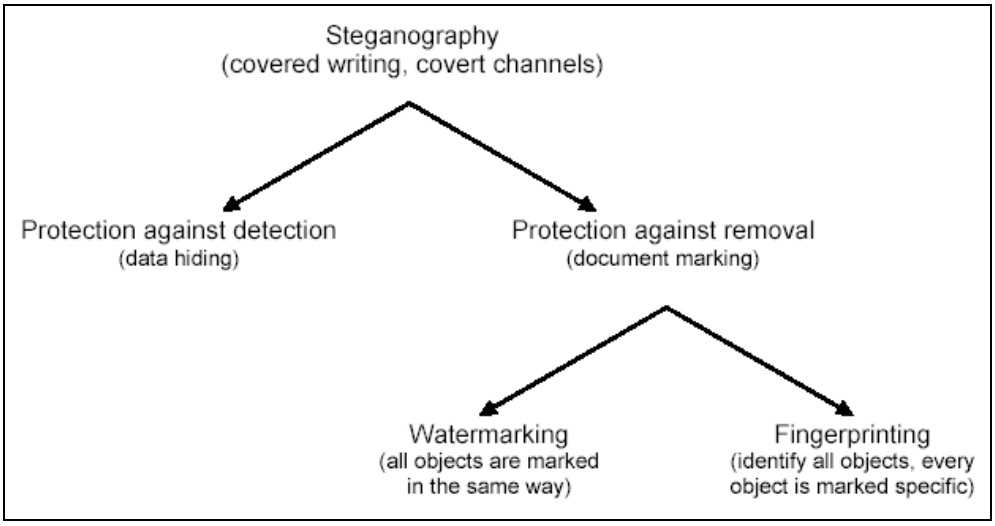
Steganografi berasal dari bahasa Yunani yang artinya untuk tulisan yang disembunyikan.

Steganografi merupakan proses penyembunyian data rahasia ke dalam data lainnya. Data yang menjadi media merupakan data yang umum dikirimkan, bisa berupa teks, gambar, audio, maupun video. Data yang dijadikan media untuk menyembunyikan pesan disebut *cover medium*. *Cover medium* yang telah ditambahkan pesan rahasia dengan steganografi disebut stego data. Pada keadaan yang ideal, siapapun yang melakukan *scan* terhadap data tersebut tidak akan mengetahui bahwa data tersebut mengandung data lain yang rahasia sehingga pengambilan data hanya dapat dilakukan oleh penerima yang berhak.

Enkripsi dan stegnografi mempunyai tujuan yang berbeda. Enkripsi menyandikan data sedemikian sehingga penerima yang tidak diharapkan tidak dapat mengetahui artinya. Steganografi, sebaliknya, tidak mengubah data menjadi tidak berguna bagi penerima yang tidak diharapkan. Tetapi, steganografi bertujuan mencegah agar orang-orang selain penerima yang berhak tidak menyadari bahwa data tersebut ada.

Banyaknya teknik dalam steganografi menyebabkan diperlukan adanya pengelompokan atas jenis-jenisnya. Pengelompokan ini diharapkan akan memudahkan pengguna steganografi untuk memilih teknik yang sesuai dan pembuat steganografi untuk mengembangkan teknik-teknik baru dengan lebih terarah.

Steganografi sendiri sering dibedakan menjadi dua jenis menurut tujuannya, yaitu steganografi untuk menghindari deteksi (*data hiding*) dan steganografi untuk menghindari penghapusan data (*document marking*). Jenis pertama kemudian lebih sering disebut sebagai steganografi itu sendiri. Jenis kedua dibagi lagi menjadi dua yaitu *watermarking* dan *fingerprinting*. *Watermarking* lebih banyak dibahas bersama dengan steganografi.



Gambar 1. Penggolongan Steganografi

Manfaat utama dari *watermarking* adalah untuk identifikasi dan menyertakan potongan informasi yang unik pada suatu media tanpa disadari orang lain. Kedua hal tersebut umumnya ditujukan untuk menandakan keaslian dari suatu karya yang pada akhirnya bisa meminimalkan tindak pembajakan atas karya tersebut. Hingga saat ini semakin banyak perusahaan yang memanfaatkan *watermarking*.

2.2. Sejarah Steganografi

Salah satu penerapan steganografi yang paling awal telah dicatat dalam sejarah. Pada abad ke-11 Cina, seorang diplomat menuliskan pesan pada lembaran sutra yang tipis kemudian menggulungnya kedalam sebuah bola kecil. Bola seperti ini mudah disebunyikan dan digelindingkan.

Kisah lainnya disampaikan oleh Herodotus sekitar tahun 440 Sebelum Masehi. Histiaeus mencukur kepala budak kepercayaannya dan mentatonya dengan pesan yang menjadi tidak terlihat ketika rambutnya tumbuh kembali. Budak tersebut dikirim ketika rambutnya telah tumbuh. Pesan tersebut disampaikan kepada rekannya yang berada cukup jauh. Cara tersebut dilakukan untuk menghindari isi pesan diketahui oleh pihak yang tidak diinginkan di tengah perjalanannya.

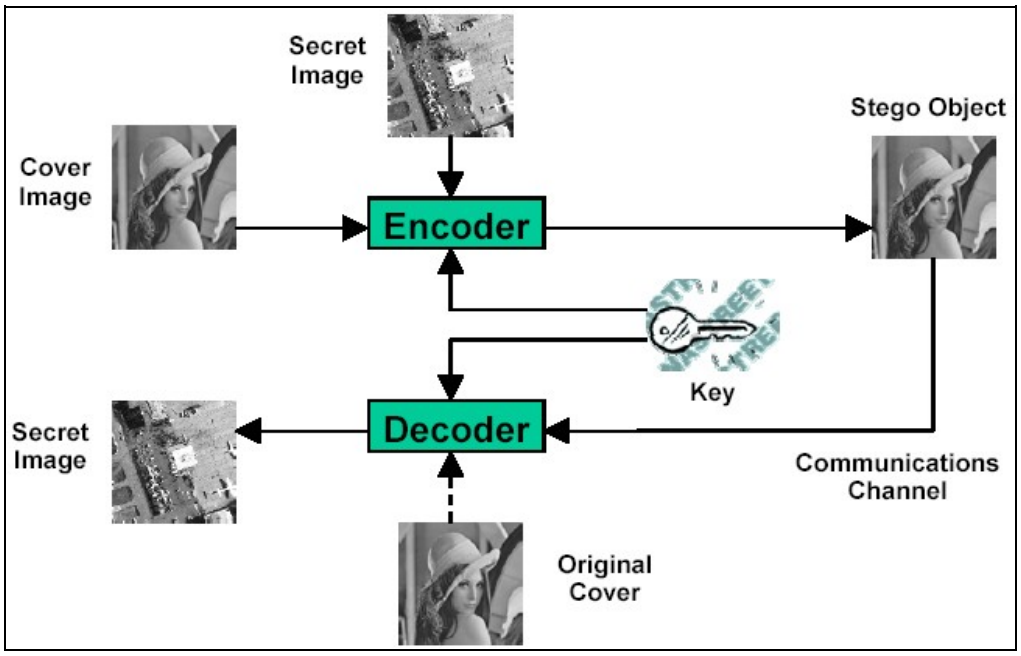
Selama revolusi Amerika, tinta tidak terlihat yang akan berkilau dalam gelap digunakan oleh pihak Inggris dan Amerika untuk berkomunikasi secara rahasia.

Steganografi juga digunakan dalam Perang Dunia pertama dan kedua. Jerman menuliskan teks rahasia dengan menggunakan tinta tidak terlihat untuk mencetak titik kecil di atas atau di bawah huruf-huruf dan dengan mengubah ketinggian dari huruf-huruf pada teks yang menutupi pesan.

Salah satu pesan yang dikirim oleh Jerman pada Perang Dunia II berisi:
"Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects for pretext embargo on by-products, ejecting suets and vegetable oils."
Dengan mengambil huruf kedua dari masing-masing kata, pesan rahasia yang berbunyi "*Pershing sails for NY June 1*" bisa didapat.

2.3. Penerapan Steganografi

Steganografi modern bertujuan untuk mempertahankan keberadaan pesan rahasia tidak terdeteksi, tetapi sistem stenografi seringkali meninggalkan jejak yang bisa dideteksi pada *cover medium*. Karena itu digunakan tambahan informasi rahasia pada steganografi modern yang disebut sebagai kunci.



Gambar 2. Skema Steganografi

Steganografi modern diharapkan hanya bisa terdeteksi apabila kunci rahasia tersebut diketahui. Dalam steganografi, untuk mempertahankan agar tetap tidak terdeteksi, *cover medium* asli yang belum dilapisi pesan rahasia harus dijaga kerahasiaannya. Apabila *cover medium* yang asli pernah diperlihatkan kepada orang lain, *cover medium* yang asli tersebut bisa dibandingkan dengan *cover medium* yang telah menjadi *stego data* dan perbedaannya akan terlihat. Pada gambar, *cover image* yang telah dilapisi data rahasia akan berubah warnanya walaupun tidak selalu terlihat jelas.

Pada steganografi digital modern, data dimasukkan ke dalam data redundan (data yang tersedia tetapi seringkali tidak diperlukan), seperti *field* pada protokol komunikasi, gambar grafik, dan sebagainya.

3. *Voice over Internet Protocol*

3.1. Pengertian dari *Voice over Internet Protocol*

Voice over Internet Protocol sering disebut sebagai *VoIP*, *IP Telephony*, *Internet telephony*, *Broadband telephony*, *Broadband Phone*, dan *Voice over Broadband*.

Kata "*VoIP*" mendeskripsikan kompresi dengan digitalisasi dan pengiriman sinyal audio analog dari seorang pengirim kepada seorang penerima menggunakan paket-paket IP.

VoIP merupakan *routing* dari percakapan dengan suara pada internet atau melalui protokol internet (IP) berbasis jaringan lainnya. Protokol yang digunakan untuk membawa sinyal suara melalui jaringan IP disebut sebagai *Voice over IP* atau *VoIP protocols*.

VoIP bisa dikatakan sebagai perwujudan dari eksperimen *Network Voice Protocol* yang dilakukan oleh perusahaan penyedia layanan Yang bernama ARPANET. Sejumlah biaya digunakan untuk menjalankan sebuah jaringan tunggal untuk membawa suara dan data. Apabila pengguna telah mempunyai kapasitas jaringan yang dapat digunakan untuk VoIP, mereka tidak perlu mengeluarkan biaya tambahan.

3.2. Penerapan VoIP

VoIP mampu memfasilitasi pekerjaan-pekerjaan yang mungkin saja lebih sulit dilakukan dengan menggunakan jaringan telepon tradisional. Pekerjaan-pekerjaan tersebut antara lain:

- Dalam pengiriman data suara dengan VoIP, ukuran dari jaringan yang digunakan dan jarak antara pelaku komunikasi tidak memberikan banyak

pengaruh. Panggilan masuk dapat dirutekan ke dalam *VoIP phone* penerima secara otomatis, tanpa dipengaruhi dari mana si penerima terhubung ke dalam jaringan. Karena itu *VoIP phone* dapat dibawa selama perjalanan. Dimanapun penggunanya terhubung dengan internet, dia bisa menerima panggilan masuk. Artinya, VoIP bisa dan telah menjadi penghubung yang menjangkau seluruh dunia.

- Nomor telepon gratis untuk digunakan dengan *VoIP* telah tersedia di Amerika Serikat, Inggris, dan negara-negara lain yang tergabung dalam perkumpulan pengguna *VoIP*.
- Pusat pengelola panggilan dengan menggunakan VoIP dapat bekerja dari manapun asalkan tersedia koneksi internet yang memadai dalam hal kecepatan dan kestabilan.
- Banyak paket-paket VoIP yang menyediakan fitur-fitur *PSTN* yang biasanya dikenakan biaya pemakaian oleh *PSTN* tersebut atau bahkan tidak disediakan oleh perusahaan telekomunikasi lokal, seperti obrolan tiga arah, penekanan ulang nomor secara otomatis, informasi identitas penelpon, dan *call forwarding*.

VoIP untuk panggilan telepon VoIP melalui perusahaan penyedia layanan manapun biasanya gratis, sedangkan VoIP untuk panggilan melalui PSTN umumnya mengenakan biaya kepada pengguna VoIP.

Ada dua jenis *PSTN* untuk layanan VoIP, yaitu: *DID* (*Direct Inward Dialing*) dan *access numbers*. *DID* akan menghubungkan penelepon secara langsung kepada pengguna VoIP, sedangkan access numbers meminta penelepon untuk memasukkan nomor ekstensi dari pengguna VoIP. Penelepon melalui *access numbers* biasanya akan dikenakan biaya telepon lokal dan pengguna VoIP tidak dikenakan biaya. *DID* biasanya mempunyai iuran bulanan, tetapi ada juga yang gratis bagi pengguna VoIP. Biaya hanya dikenakan bagi penelepon.
Dalam VoIP, data suara yang dikirimkan dipecah menjadi beberpa paket IP. Dalam keadaan yang ideal, paket-paket tersebut dikirimkan kepada penerima sesuai dengan urutannya dan sampai dengan waktu yang konstan. Ketika menerima rangkaian pesan, penerima menjalankan proses yang berkebalikan untuk mendapatkan sinyal suara dengan susunan yang seharusnya. Setelah itu penerima bisa menjadi pengirim pesan.

VoIP dengan jaringan TCP/IP, yang memberikan layanan real-time, menggunakan RTP (Real-Time Protocol) dengan UDP (User Datagram Protocol) untuk menyalurkan aliran data digital. Saat ini terdapat satu protokol pengendali untuk RTP yaitu RTCP (Real-Time Control Protocol). Protokol ini didesain untuk mengawasi kualitas layanan pengiriman data dan untuk menyampaikan informasi mengenai pihak-pihak yang terlibat dalam sesi yang sedang berjalan.

Karena UDP tidak menyediakan mekanisme untuk memastikan bahwa paket-paket data telah terkirim dengan urutan yang benar, atau untuk menyediakan jaminan atas kualitas layanan, implementasi dari VoIP menghadapi tantangan dalam mengatasi latensi jaringan dan variasi penundaan pengiriman paket-paket data. Hal ini terutama terjadi ketika sirkuit satelit terlibat di dalamnya karena terdapatnya penundaan perambatan akibat perputaran yang panjang (400 milliseconds sampai 600 milliseconds untuk satelit geostationary). Simpul yang menerima harus menyusun kembali paket-paket IP yang mungkin saja melebihi batas, tertunda, atau hilang, sambil memastikan konsistensi waktu aliran suara yang sesuai. Fungsi ini biasanya dijalankan dengan alat bernama *jitter buffer*.

Tantangan yang dihadapi oleh VoIP antara lain adalah adanya kemungkinan-kemungkinan penundaan atau latensi jaringan, hilangnya sebagian paket data, variasi waktu penundaan pengaliran paket-paket data, pengulangan (*echo*), dan keamanan.

Tantangan lain adalah merutekan lalu lintas VoIP melalui *firewalls* dan *address translator* (penerjemah alamat). *Session Border Controllers* pribadi digunakan sepanjang *firewalls* untuk mengaktifkan panggilan VoIP kepada dan dari jaringan perusahaan yang diproteksi.

Dari semua tantangan yang dihadapi oleh VoIP, secara umum terdapat dua hal yang paling sulit untuk diwujudkan yaitu kualitas pelayanan dan keamanan.

Dalam hal keamanan, perlu diketahui bahwa terdapat banyak kemungkinan serangan terhadap komunikasi dengan VoIP. Serangan-serang tersebut di antaranya adalah sebagai berikut:

- *Direct Access Over the Network*.
  Jika terjadi telepon melalui jaringan, bisa saja beberapa fungsinya diakses oleh pihak lain melalui jaringan
- *Network Sniffing*.
  Infrastuktur telepon awalnya didesain untuk menciptakan sebuah sambungan titik ke titik antara penelepon dan penerimanya, dengan asumsi tidak akan ada pihak ketiga pada jalur tersebut. Jaringan pengiriman paket data didesain untuk mengirim data melalui jalur yang dapat diakses oleh siapapun. Sinyal apapun yang dikirim tanpa melalui proses enkripsi atau proses lainnya harus diasumsikan dapat diakses oleh siapapun, walaupun tanpa akses fisik secara langsung seperti melalui *PSTN*.
- *Data Exfiltration.*
  Lalu lintas pada VoIP traffic membutuhkan bandwidth yang lebar untuk menjalankan penjagaan dan firewalls, agar tidak terjadi penundaan yang terlalu lama. Paket-paket VoIP, tidak seperti paket-paket data lain yang diketahui formatnya, akan sangat sulit (bahkan tidak mungkin) untuk melakukan scan terhadap data yang tidak diharapkan atau data yang tersembunyi tanpa menyebabkan penundaan yang memakan waktu. Jika tidak ditemukan alat untuk memisahkan lalu lintas VoIP dari lalu lintas data lainnya, VoIP sangat mungkin menjadi kendaraan bagi trojan horse atau penyusupan data lainnya yang akan merugikan.
- *Control/Signaling Attacks*.
  Jaringan data modern seringkali menjalankan kontrol dan sinyal data melalui jalur umum. Hal ini juga memungkinkan bagi jaringan telepon konvensional, tetapi dengan adanya pembatasan akses ke dalam sistem yang tersambung, jaringan telepon relatif lebih aman.
- *Protocol-Based Attacks*.
  Karena VoIP relatif baru, belum dapat terlihat akibat dari adanya penyusup yang memanipulasi protokol dengan cara yang tidak terpikirkan sebelumnya. Analisis lebih dalam terhadap protokol dan implementasinya sangat dibutuhkan untuk mengetahui kelemahan protokol terhadap buffer overflows, man-in-the-middle attacks, traffic analysis, content-based attacks, atau hal lain yang mungkin terjadi pada sistem VoIP.
- *IP Spoofing*.
  IP spoofing telah dikenal sebagai serangan terhadap data dalam jaringan, dimana seorang penyusup membajak suatu sesi, berlaku menggunakan identitas penerima. Hal ini sangat mungkin terjadi juga untuk merutekan ulang atau menyusupi lalu lintas VoIP sehingga memungkinkan terjadinya masquerade atau man-in-the-middle attacks.

4. Steganografi pada VoIP

Layanan keamanan yang paling penting untuk mengamankan sistem VoIP antara lain: otentikasi, kesatuan, dan kerahasiaan. Otentikasi dan kesatuan bisa diwujudkan dengan pemilihan protokol yang digunakan. Tetapi untuk kerahasiaan, perlu diterapkan perlakuan yang berbeda seperti penggunaan mekanisme keamanan dengan model klasik (kriptografi).

Untuk gambar-gambar digital seperti halnya suara digital, telah terdapat banyak teknik steganografi yang bisa diterapkan dan telah terdapat banyak pula pendekatan untuk mendeteksi steganografi pada gambar-gambar digital tersebut.

Bagaimanapun, untuk mendeteksi pesan tersembunyi di dalam data suara, masih sedikit metode yang telah dipublikasikan walaupun teknologi pengiriman data suara seperti VoIP menyediakan field tambahan untuk mengaplikasikan steganografi. Fields tersebut bisa digunakan sebagai *covert channel*. Selain itu pada data suara dapat juga diaplikasikan metode l*east significant bits* (LSB).

4.1. Least Significant Bits pada VoIP

LSB semula lebih banyak digunakan pada data gambar, tetapi kemudian berkembang ke data suara. Penyembunyian data pada least significant bits (LSBs) dari data suara pada domain waktu merupakan salah satu algoritma paling sederhana dengan tingkat data informasi tambahan yang sangat tinggi.

Pengkode LSB watermark biasanya memilih sebuah subset dari seluruh host suara yang mungkin dengan menggunakan sebuah kunci rahasia. Operasi substitusi pada LSB dilakukan di subset tersebut.

Proses ekstraksi dilakukan dengan membaca bit-bit yang diterima dari aliran bit suara yang diterima. Alat penerjemah memerlukan semua bagian dari data suara yang digunakan selama proses penempelan pesan rahasia.

Metode pengkodean LSB standar dengan mudah mengganti bit pada suara asli pada lapisan ke-i (i=1,…,16) dengan bit dari aliran bit data rahasia.

Algoritma LSB yang digunakan harus melakukan penempelan bit yang menimbulkan distorsi yang minimal pada suara yang ditempeli.

Salah satu algoritma yang bisa digunakan adalah sebagai berikut:

if host sample a≥0

if bit 0 is to be embedded
if a_{i-1}=0 then $a_{i-1}a_{i-2}\ldots a_0$=11…1
if a_{i-1}=1 then $a_{i-1}a_{i-2}\ldots a_0$=00…0
and
ifa_{i+1}=0 then a_{i+1}=1
else if a_{i+2}=0 then a_{i+2}=1
…
else if a_{15}=0 then a_{15}=1

else if bit 1 is to be embedded
if a_{i-1}=1 then $a_{i-1}a_{i-2}\ldots a_0$=00…0
if a_{i-1}=1 then $a_{i-1}a_{i-2}\ldots a_0$=00…0
and
ifa_{i+1}=0 then a_{i+1}=1
else if a_{i+2}=0 then a_{i+2}=1
…
else if a_{15}=0 then a_{15}=1

if host sample a<0

if bit 0 is to be embedded
if a_{i-1}=0 then $a_{i-1}a_{i-2}\ldots a_0$=11...1
if a_{i-1}=1 then $a_{i-1}a_{i-2}\ldots a_0$=00…0
and
ifa_{i+1}=1 then a_{i+1}=0
else if a_{i+2}=1 then a_{i+2}=0
…
else if a_{15}=1 then a_{15}=0

else if bit 1 is to be embedded
if a_{i-1}=1 then $a_{i-1}a_{i-2}\ldots a_0$=00…0
if a_{i-1}=0 then $a_{i-1}a_{i-2}\ldots a_0$=11...1and
ifa_{i+1}=1 then a_{i+1}=0
else if a_{i+2}=1 then a_{i+2}=0
…
else if a_{15}=1 then a_{15}=0

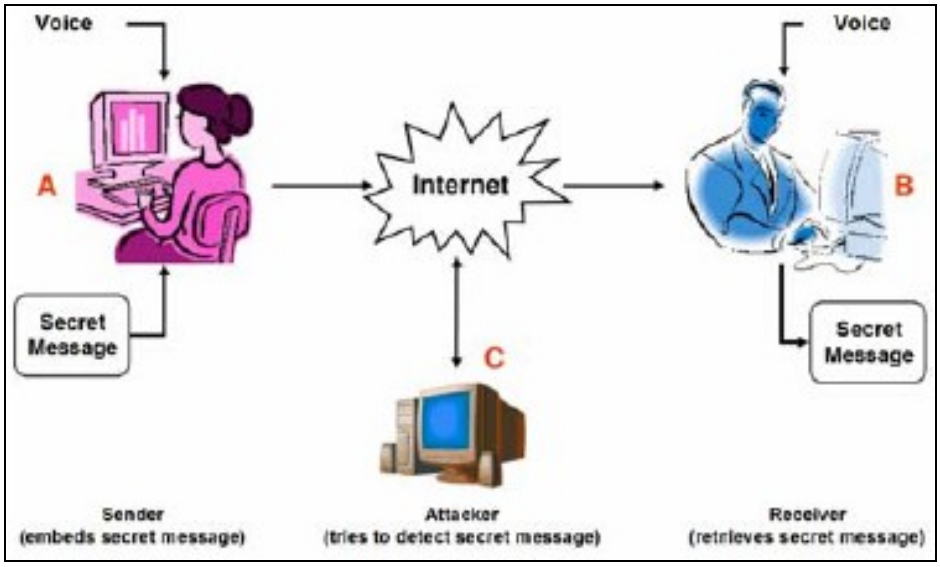
4.2. Covert Channel

Telah kita ketahui bahwa terdapat banyak ancaman keamanan terhadap komunikasi dengan VoIP.

Covert channel merupakan metode komunikasi yang bukan bagian dari desain sistem komputer aktual, tetapi dapat digunakan untuk memindahkan informasi kepada pengguna atau proses di dalam sistem yang normalnya tidak akan diizinkan mengakses informasi tersebut.

Data yang diproses memberikan informasi kebutuhan untuk adaptasi terhadap firewalls dan penjagaan dan efek pada jaringan data yang sebelumnya telah ada. Diasumsikan bahwa penyaringan tambahan atau pengawasan akan dibutuhkan untuk mendeteksi modulasi atau hal lain yang mempengaruhi aliran lalu lintas pada VoIP untuk membawa *covert data* masuk maupun keluar.

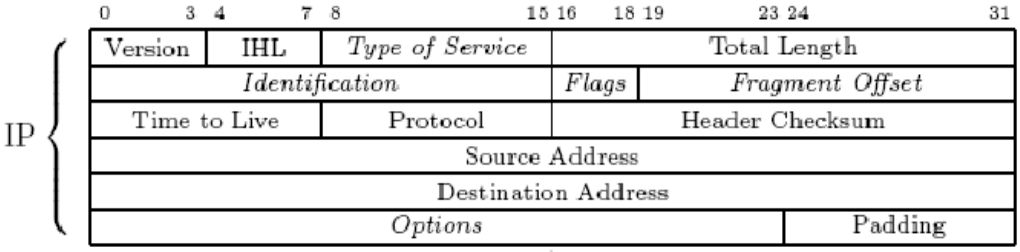
Lingkungan dari VoIP aktif dengan menggunakan channel steganografi diilustrasikan di bawah ini:



Gambar 3. Lingkungan implementasi VoIP

Alice (A) di sebelah kiri dan Bob (B) di sebelah kanan sedang melakukan percakapan pada koneksi VoIP yang tidak mencurigakan. Diasumsikan bahwa Alice sedang ingin mengirim pesan rahasia kepada Bob.

Covert channel akan digunakan untuk mentransmisikan header (control bits) paket data Header IP terdiri dari beberapa fields yang dapat digunakn sebagai sebuah covert channel. Kapasitas total dari fields tersebut mempunyai selisih 60 bits per paket. Dan terdapat field protokol UDP dan RTP yang dapat digunakan.



Gambar 4. Fields pada Header IP

Artinya Alice berlaku sebagai pengirim dan Bob sebagai penerima. Alice menempelkan pesan rahasinya pada aliran VoIP dengan menggunakan sisi rahasia yang diketahui oleh Bob tetapi tidak diketahui oleh orang lain.

Pada TCP/IP, terdapat beberapa metode yang dapat digunakan, dimana covert channels dapat diciptakan dan data dapat dipertukarkan antara host pengirim dan penerima. Sebuah analisis terhadap header protokol TCP/IP yang sering ditemui seperti IP, UDP, TCP, HTTP, ICMP memberikan hasil pada *fields* yang tidak terpakai atau opsional. Hal ini memberikan banyak kemungkinan dimana data bisa disimpan dan ditransmisikan.

Setiap PDU terdiri dari header (control bits) dan sejumlah bit data tertentu yang ditempelkan pada suara pengirim/penerima. *Fields* yang tidak digunakan atau opsional pada paket-paket IP/UDP/RTP akan digunakan karena protokol-protokol tersebut digunakan oleh sebagian besar Implementasi IP telephony. Protokol lainnya juga bisa digunakan, tidak terbatas pada protokol tersebut di atas.

Lapisan yang lebih rendah pada *TCP/IP stack* juga mempunyai kemungkinan menjadi tempat penerapan steganografi. Lebih jauh lagi, kita bisa mendistribusikan control bits pada fields tersebut dalam bentuk yang telah dideterminasikan sebelumnya (bagian ini dapat dipertukarkan selama fase pemberian sinyal pada percakapan).

Pada fields yang dipilih tersebut kita hanya akan mentransmisikan header (control bits) dari protokol yang digunakan dengan teknik steganografi. Header terdiri dari 6 bit per paket, jadi jenis transmisi seperti ini akan sulit untuk ditemukan.

Menurut sejarah, identifikasi dan pencegahan oleh covert channels merupakan salah satu masalah yang rumit dalam keamanan komputer, walaupun ketika dibatasi hanya pada data.

Kebutuhan tambahan untuk mendeteksi covert channels pada sinyal analog dasar meningkatkan tantangan proteksi secara signifikan. Masalah ini mungkin membutuhkan isolasi sistem VoIP untuk mencegah sinyal bermodulasi. Hal ini merupakan area lain dimana menggabungkan pemrosesan sinyal digital dan pembagian suatu jaringan tunggal untuk suara dan data menimbulkan risiko yang tidak muncul (atau kemungkinan kecil terjadi) pada sistem suara dan data yang terpisah.

Satu hal yang paling penting adalah pada covert channel juga dilakukan verifikasi keamanan dari sumber transmisi dan data yang dikirim (otentikasi dan kesatuan).

4. Kesimpulan

Protokol yang digunakan untuk membawa sinyal suara melalui jaringan IP disebut sebagai *Voice over IP* atau *VoIP protocols*.

Dari semua tantangan yang dihadapi oleh VoIP, secara umum terdapat dua hal yang paling sulit untuk diwujudkan yaitu kualitas pelayanan (meliputi: penundaan atau latensi jaringan, variasi waktu penundaan pengaliran paket-paket data, hilangnya sebagian paket data) dan keamanan.

Dalam hal keamanan, komunikasi dengan VoIP cenderung mudah untuk disusupi. Untuk itu diperlukan metode untuk memberikan keamanan bagi pengguna VoIP.

Steganografi merupakan proses penyembunyian data rahasia ke dalam data lainnya. Data yang menjadi media merupakan data yang umum dikirimkan, bisa berupa teks, gambar, audio, maupun video.

Untuk mendeteksi pesan tersembunyi di dalam data suara, masih sedikit metode yang telah dipublikasikan walaupun teknologi pengiriman data suara seperti VoIP menyediakan field tambahan untuk mengaplikasikan steganografi.

Dua contoh aplikasi steganografi pada VoIP adalah dengan LSB dan *covert channel*.

LSB semula lebih banyak digunakan pada data gambar, tetapi kemudian berkembang ke data suara. Pengkode LSB biasanya memilih sebuah subset dari seluruh host suara yang mungkin dengan menggunakan sebuah kunci rahasia.

Operasi substitusi pada LSB dilakukan di subset tersebut. Algoritma LSB yang digunakan harus melakukan penempelan bit yang menimbulkan distorsi yang minimal pada suara yang ditempeli.

Pada TCP/IP, terdapat beberapa metode yang dapat digunakan, dimana covert channels dapat diciptakan dan data dapat dipertukarkan antara host pengirim dan penerima.

Pada protokol TCP/IP yang sering ditemui seperti IP, UDP, TCP, HTTP, ICMP terdapat *fields* yang tidak terpakai atau opsional. Hal ini memberikan banyak kemungkinan dimana data bisa disimpan dan ditransmisikan. Fields tersebut bisa digunakan sebagai *covert channel*.

LSB dan covert channel tidak memakan bandwidth karena control bits (header dari protokol yang baru) ditransmisikan pada covert (steganografik) channel dan data tidak terpisah dari suara asli.

Menempelkan pesan tersembunyi pada komunikasi dengan VoIP merupakan pekerjaan yang menarik dan dapat menjadi studi yang akan dibahas lebih banyak lagi.

Daftar Pustaka

[1] Security for Voice Over Internet Protocol, IATF Release 3.ÌSeptember 2002

[2] Jana Dittmann, Thomas Vogel, and Reyk Hillert, Design and Evaluation of Steganography for Voice-over-IP, http://wwwiti.cs.uni-magdeburg.de

[3] http://id.wikipedia.org/wiki/Voice_over_IP

[4] Wojciech Mazurczyk1 and Zbigniew Kotulski, New security and control protocol for VoIP based on steganography and digital watermarking, Warsaw University of Technology, Faculty of Electronics and Information Technology, Institute of Telecommunications

[5] Nedeljko Cvejic, Tapio Seppänen, Increasing Robustness of LSB Audio Steganography Using a Novel Embedding Method, IEEE, Proceedings of the International Conference on Information Technology: Coding and Computing, 2004