TEKNIK PEMBANGKITAN KUNCI MENGGUNAKAN SUARA

Risa Astari Dewi – NIM : 13506064

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if16064@students.if.itb.ac.id

Abstrak

Makalah ini membahas teknik pembangkitan kunci melalui pengenalan suara. Ide penggunaan suara diadaptasi dari penggunaan *biometrics* manusia lainnya, seperti cap jari dan iris mata. Dengan asumsi tiap orang akan memiliki karakteristik suara yang berbeda. Pada penerapannya, kata kunci diucapkan oleh pengguna. Kemudian oleh mesin atau perangkat, suara akan dikenali dan dibandingkan dengan data suara yang telah disimpan sebelumnya.

Penggunaan *biometrics* secara umum sendiri untuk menutupi kelemahan dari kritografi sejak lama, dalam hal memilih dan mengingat kata kunci. Pembahasan akan didukung alasan pemilihan *biometrics* suara diantara *biometrics* lainnya. Diberikan pula kriteria yang menunjang penerapan teknik ini agar lebih sempurna.

Teknik pengimplementasiannya menggunakan *feature descriptor* yang akan mengubah hasil pengucapan kata. Proses komputasi lebih lanjut akan dikenakan pada masukan suara hingga didapat bit string.

***Kata kunci**: voice recognition, generate key, biometrics*

1. Pendahuluan

Dalam penerapan kriptografi telah lazim menggunakan suatu kunci sebagai penanda hak otorisasi data. Ketika kunci teruji valid, maka hak akses ke data akan diberikan. Pada kriptografi modern yang menerapkan sistem digital kunci biasanya merupakan rangkaian interger atau karakter tertentu yang bisa dimasukan dari keyboard. Namun ketidakmampuan pengguna untuk mengingat kuat kunci telah menjadi kelemahan dalam kriptografi. Terdapat kecenderungan bahwa pengguna memilih sandi yang singkat dan mudah ditebak jika mereka lupa kuncinya. Timbul persoalan ketika penyerang mampu menebak kunci dengan mengetahui kebiasaan pengguna. Sehingga muncul teknik kriptografi baru yang memanfaatkan keunikan dari manusia. Misalkan cap jari atau pemindaian iris mata. Teknik ini didasarkan dengan asumsi tiap manusia memiliki karakteristik yang berbeda, tidak ada 2 orang yang memiliki cap jari atau iris mata yang sama.

Dengan memanfaatkan asumsi yang sama, keunikan suara bisa digunakan untuk membangkitkan kata kunci. Idenya adalah data tentang karakteristik suara telah dicirikan dan disimpan telebih dahulu, ketika pengguna mengucapkan sandi, mesin akan mengenali suara dan melakukan perbandingan dengan data yang tersimpan. Karakteristik yang dikenali dari suara adalah kata sandi tertentu dan artikulasi berikut intonasi pengguna saat mengucapkannya. Dengan asumsi suara manusia unik, maka tiap orang akan memiliki artikulasi dan intonasi yang berbeda.

2. Pemilihan *biometrics* suara

Ada beberapa tanda lahir manusia yang bisa menjadi otentifikasi, oleh ilmuwan dikenal dengan *biometrics* manusia. Terdapat beberapa alasan yang mendukung pemilihan teknik *biometrics* suara :

- Pertama, merupakan cara komunikasi yang akrab, hal ini membuatnya ideal pada beberapa aplikasi. Contohnya *voice activated phones*, *voice dialing* adalah aplikasi yang telah banyak digunakan dimasyarakat. Pengguna telepon cukup mengucapkan nomor tujuan, mesin akan mengenali suara dan menghubungi nomor tersebut.
- Kedua, penelitian tentang verifikasi suara telah menunjukan suara mampu membedakan pengguna dengan efektif. Penelitian ini didukung dengan banyaknya mesin dan aplikasi yang berbasis pengenalan suara (voice recognition).

- Ketiga, saat seseorang ingin mengubah kata kuncinya, akan sulit untuk mengubah artikulasi dari sandi. Dengan demikian, berbeda dari *biometrics* statik (cap jari, iris mata) yang mungkin akan selalu sama sepanjang masa.

Penggunaan suara tidak akan terbatas. Selama penyerang tidak mengetahui kata kunci yang dimaksudkan, atau bahkan jika diketahui mesin akan mengenalinya dari artikulasi kata. Namun, masih beresiko ketika penyerang mampu merekam kata kunci saat diucapkan oleh pengguna. Untuk hal ini ada cara menanggulanginya yang akan dibahas.

3. Kriteria

Biometrics suara memang cukup rentan untuk digunakan tapi mampu memberikan tingkat keamanan yang sebanding. Agar teknik ini bisa memberikan hasil yang maksimal, dibutuhkan kriteria untuk memenuhi standar penggunaan suara:

- Perangkat yang mampu mengenali suara. Melalui perangkat inilah suara akan dianalisa untuk mendapatkan data karakteristik yang akan disimpan
- Lingkungan yang mendukung. Meliputi tingkat kebisingan disekitar perangkat. Misalkan saat kata kunci diucapkan, tidak ada suara tambahan lainnya (seperti suara mobil, percakapan dll). Kondisi terbaik bisa dicapai jika perangkat diposisikan di dalam ruangan yang memungkinkan tidak ada suara gangguan.
- Artikulasi yang jelas. Mungkin dalam hal aksen atau intonasi, seseorang akan selalu sama. tapi artikulasi dari kata cukup rentan. Seseorang dengan kondisi sehat akan memiliki artikulasi yang berbeda dengan orang yang terkena flu atau penyakit sejenis yang menyebabkan terjadinya perubahan suara.

Diluar dari pemenuhan kriteria tersebut, penyerang (attacker) bisa saja melakukan analisa secara brute force. Karena pada dasarnya suara akan dikenali dari bit yang dihasilkan. Maka ditambah satu kriteria lagi, panjang kunci yang diucapkan memadai sehingga bisa didapat 56-bit. Bit ini kemudian dikenakan metode DES untuk memperkuat kunci.

Nantinya sistem pengenalan suara akan terdiri dari:

- Microphone, alat penangkap suara
- Perangkat lunak pengenal suara
- Komputer yang menginterpretasikan pengucapan
- *Soundcard* berkualitas untuk masukan dan keluaran.

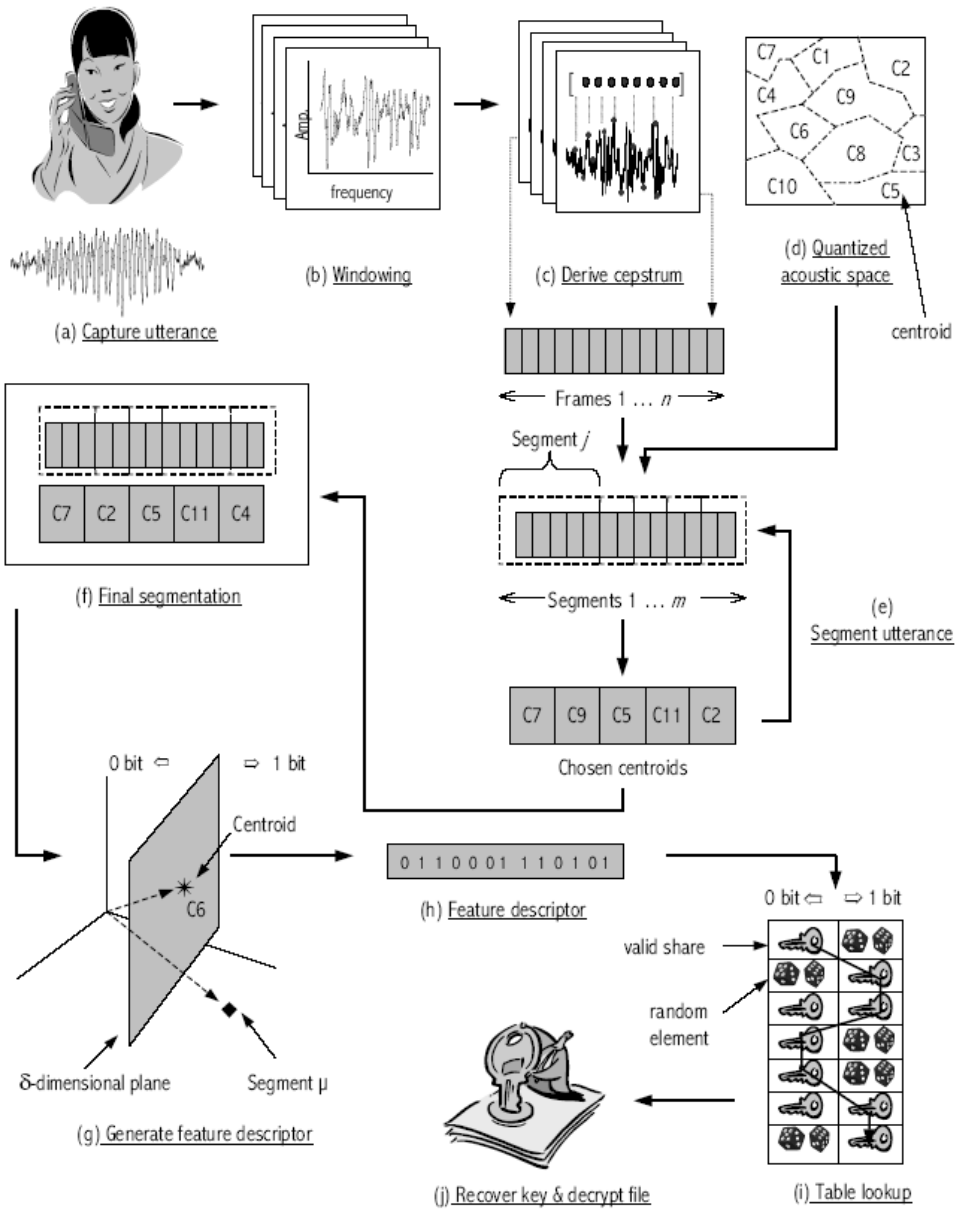
4. Implementasi

Teknik ini telah diterapkan sebelumnya oleh militer Amerika pada secure telephone (jaringan telepon terjaga). Pengguna mengucapkan kata kunci untuk membangkitkan kunci. Kunci inilah yang kemudian digunakan untuk men-dekrip suara yang diterima ditelepon. Tentu saja suara penelpon telah dienkripsi dahulu.

Teknik kriptografi yang menggunakan *biometrics* memiliki 2 tahapan umum. Tahap pertama adalah mengenali masukan mentah yang diterima oleh perangkat pengukuran *biometrics*, yang dikenal dengan *feature descriptor*. Perangkat ini akan melakukan pengujian dan komputasi pada masukan hingga didapat m-bit string data. Hasil yang didapat menjadi masukan pada tahap selanjutnya. Ditahap kedua yang akan menghasilkan kunci kriptogafi, membandingkan hasil *feature descriptor* dengan data yang telah tersimpan sebelumnya. Jika keduanya sama, maka kunci kriptografi yang sama akan dihasilkan dari keduanya.

Masukan suara yang didapat akan disegmentasi kedalam frame. Mengutip dari penelitian tentang pengenalan suara menyebutkan *feature descriptor* memulai segmentasi dengan model akustic.

Data yang telah terbagi menjadi beberapa segmen ini akan dilakukan pembangkitan *feature descriptor*nya untuk setiap segmen berdasarkan centroid dari setiap segmen. Hasil dari *feature descriptor* ini akan berupa deretan bit yang akan digunakan untuk membangkitkan kunci yang dibutuhkan untuk mendekripsi dan enkripsi file di dalam table lookup. Kunci yang di dapat inilah yang akan digunakan unuk mengenkripsi dan dekripsi file yang diinginkan.



Gambar 1 Pembangkitan kunci menggunakan suara

Salah satu kelemahan teknik ini adalah dalam hal keakuratan mesin dalam menangkap suara masukan. Sangat sulit mengukur ketepatan berbicara bagi sistem. Ada faktor teknis dan manusia yang ikut terlibat di dalamnya. Masalah yang serupa juga ditemukan pada teknik yang memanfaatkan biometrics lainnya.

Dari hasil ujicoba terhadap sistem pengenalan suara menunjukkan skor sekitar 95% akurasi yang dapat dilakukan dengan peningkatan jumlah sistem. Misalnya, dalam percobaan yang melibatkan pendiktean koran, cerita, pesan email dan surat bisnis, Dragon NaturallySpeaking 6,0 angka 95% akurasi, ViaVoice angka akurasi 92% NaturallySpeaking dan hanya 5,0 angka akurasi 85%. Ketiga sistem ini adalah sistem pengenalan suara yang telah dikenal umum.

Pendekatan terbaru yang ditawarkan oleh sistem adalah dibangunnya sistem pakar kosakata. Langkah ini sangat bermanfaat bila subjek pengguna dan kata spesifik dan akronim kemungkinan yang akan digunakan.

Pengurangan inteferensi faktor luar juga harus dilakukan.

- Menggunakan tinggi kinerja komputer. Jika menggunakan kontemporer bicara pengakuan perangkat lunak, komputer biasanya akan perlu berisi prosesor yang cepat dan besar jumlah RAM untuk bekerja secara efisien. Walaupun sering kemasan perangkat lunak menyatakan bahwa ia akan berjalan di "64MB RAM", hal ini telah sering ditemukan menjadi tidak memadai, dihasilkan dalam waktu lebih lama pelatihan 7. 256MB RAM minimum lebih baik, yang dapat menimbulkan masalah di sekolah, akademi dan perguruan tinggi yangmenggunakan komputer tua.
- Menggunakan *microphone* berkualitas baik. Microphone dengan fitur ”Active Noise Reduction” atau ”Active Noise Cancelation” bisa mereduksi suara bising dari lingkungan.
- Instalasi *soundcard*. *Soundcard* yang biasa terinstal memiliki kualitas yang beragam. Untuk sistem pengenalan suara yang serius, direkomendasikan *soundcard* yang *high quality duplex* (rekomendasi lainnya bisa dilihat di internet)
- Bekerja pada lingkungan yang hening. Walaupun penanganan kejernihan suara bisa ditangani oleh perangkat keras, faktor lingkungan tetap menjadi pengaruh besar. Sebaiknya perangkat penangkap suara diletakan di ruangan khusus.
- Menggunakan sistem operasi yang tepat. Beberapa sistem pengenalan suara yang telah dikembangkan didesain hanya pada sistem operasi tertentu. Sebelum melakukan instalasi sistem perlu dipertimbangkan sistem operasi yang digunakan sejalan dengan perangkat keras yang dipakai.

5. Kesimpulan

Suara bisa menjadi salah satu alternatif pembangkitan kunci kriptografi. Hal ini bisa menutupi keterbatasan dan kelemahan teknik pembangkitan kunci lainnya. Namun untuk implementasi secara sempurna dibutuhkan teknologi pendukung yang tinggi. Teknik ini kurang sesuai jika diterapkan pada pemakaian sederhana, lebih tepat untuk penjagaan keamanan di perkantoran atau perusahaan dimana teknologi tidak menjadi batasan.

DAFTAR PUSTAKA

[1] B. S. Atal. Automatic recognition of speakers from their voices. *Proceedings of the IEEE*, 64:460–475, 1976.

[2] Monrose, Reiter, Li & Wetzel. Cryptography Key Generation from Voice. Bell Labs, Lucent Technologies, Murray Hill, New Jersey,USA. ffabian,reiter,qli,sgwetzelg@research.bell-labs.com

[3] Kirriemuir, John. Speech Recognition Technologies. 2003. www.ceangal.com