DESAIN DAN IMPLEMENTASI ENKRIPSI SINYAL AUDIO MENGGUNAKAN BAKER MAP

Qoury Febriana[1], Koredianto Usman[2], Linda Meylani[3]

[1]Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

Abstrak

Kerahasiaan data sudah menjadi suatu bahan penelitian yang banyak dikembangkan dalam proses pengiriman informasi. Data audio digital yang tidak terkompresi umumnya mempunyai ukuran yang relatif besar. Oleh karena itu, dibutuhkan metoda yang sesuai agar proses enkripsi cepat namun kerahasiaannya pun tetap terjamin dan tingkat ketahanan yang baik terhadap serangan dari pihak luar.

Tugas akhir adalah melakukan enkripsi pada sinyal audio dengan menggunakan metoda Baker Map, yaitu dengan cara mengacak organisasi matrik aslinya. Enkripsi pada Baker Map ini secara aslinya digunakan untuk enkripsi citra yang telah diketahui kehandalannya. Dari hasil perhitungan brute force attact dengan menggunakan matrik file audio (yang diresize ke 256x256) untuk proses cracker-nya dibutuhkan waktu 1,66 x1055 tahun maka dapat dinyatakan enkripsi dengan algoritma Baker Map ini aman.

Sedangkan dari percobaan untuk mengukur waktu komputasi, untuk ukuran matrik MxM (M= 256,512, atau 1024), enkripsi dengan metoda Baker Map menggunakan variasi kunci acak masing-masing membutuhkan waktu 1.04 detik, 23.19 detik dan 185.81 detik. Proses enkripsi dan dekripsi dengan menggunakan variasi kunci acak memiliki waktu proses 6.67% lebih cepat dibandingkan dengan menggunakan variasi kunci konstan. Enkripsi klasik DES dengan ukuran file yang sama memiliki waktu komputasi masing-masing sebesar 3.39 detik, 205.98 detik dan 3290.48 detik.

Kata Kunci : Metoda Baker Map,Sinyal Audio, Brute Force Attact, Kriptografi.

Abstract

Data confidentiality has been researched in depth in various resources as a method in securing information during transmission. Uncompress audio data normally has a relatively big data size. This condition makes data encryption for audio need to be special.

In this research we use Baker Map algorithm to encrypt audio signal. Baker map is originally popular in image encryption due to its realibility. Brute force attack computation as calculated gave 1.66 x 1055 year to crack the code, hence it is safe enough to call it secure.

In term of computation time, Baker Map on audio gave computation time of 1.049, 23.10 and 185.81 seconds for audio matrix size of 256, 512 and 1024 respectively. As additional information, encryption using random key produce computation time 6,67% faster than computation using constant key. In contrary, DES algorithm produce computation time of 3.39, 205.98, 3290.48 seconds for similar matrix size.

Keywords : Brute Force Attact, Baker Map method, audio digital, DES method.

BAB I
PENDAHULUAN

1.1 Latar Belakang

Masalah keamanan merupakan salah satu aspek penting dari suatu sistem informasi. Salah satu cara pembatasan akses data bagi pihak-pihak yang tidak berhak yaitu dengan enkripsi. Enkripsi adalah proses mengkonversi pesan (*plaintext*) ke dalam bentuk *cryptogram* atau *ciphertext*. Proses ini dapat secara *software* atau *hardware* serta memerlukan *key* untuk menjalankan algoritma *Cipher* kemudian di deskripsi oleh sisi penerima dengan perangkat dan *key* yang bertipe sama, guna mendapatkan kembali *plaintext* semula.

Beberapa alasan pengguna enkripsi yaitu mencegah mereka yang tidak berwenang melihat data-data sensitif, mengurangi kemungkinan terbukanya data rahasia tanpa sengaja, mencegah mereka yang mempunyai akses istimewa agar tidak dapat melihat data pribadi dan untuk mempersulit usaha penyusup memasuki sistem.

Data yang akan dienkripsi pada tugas akhir ini adalah berupa audio digital yang tidak terkompresi. Audio digital yang akan diproses mempunyai tingkat kesulitan yang lebih kompleks dikarenakan dari ukuran matrik yang besar. Sehingga dibutuhkan metode enkripsi yang mampu menangani masalah tersebut dengan waktu proses yang cepat dan memiliki tingkat sekuritas yang tinggi terhadap serangan dari pihak yang tidak diinginkan.

Pada tugas akhir ini metode enkripsi yang digunakan adalah metode *chaotic-map*. Adapun metode *chaotic-map* yang digunakan adalah *Baker Map*. Algoritma Baker Map ini adalah algoritma yang cepat untuk citra karena kecepatannya inilah diusulkan untuk audio.[1] [2] Pada pengimplementasiannya metode ini akan dibandingkan dengan metode *DES*.

Dengan membandingkan kedua metode tersebut, diharapkan sistem dari metode *Baker Map* mampu melakukan proses enkripsi dengan waktu yang cepat dan tingkat sekuritas yang baik. Sehingga data yang dikirimkan akan tetap terjaga kerahasiannya sampai diterima oleh penerima tanpa diketahui oleh pihak luar.

1.2 Tujuan

Tujuan dari penulisan Tugas Akhir ini adalah :

- Mendesain dan mengimplementasikan enkripsi sinyal audio dengan menggunakan algoritma *Baker Map*.
- Menguji tingkat keamanan dan kecepatan proses dari metoda *Baker Map*.
- Menguji tingkat waktu komputasi terhadap fungsi dari variasi kunci.
- Menganalisa performansi dari sistem enkripsi dilihat dari kecepatan proses dan tingkat keamanannya.
- Membandingkan hasil analisis menggunakan metoda *Baker Map* dengan metoda enkripsi klasik *DES*.

1.3 Rumusan Masalah

Beberapa permasalahan pada tugas akhir dapat didefinisikan sebagai berikut :

1. Proses enkripsi sinyal audio membutuhkan suatu algoritma yang mampu mengatasi *file* dengan ukuran yang besar.

2. Algoritma *Baker Map* memiliki kelebihan dalam hal kecepatan dengan data yang berukuran besar.

1.4 Batasan Masalah

Agar pembahasan dalam Tugas Akhir ini tetap terarah pada tujuan pokoknya, maka perlu dilakukan beberapa pembatasan terhadap permasalahannya, yaitu :

1. Informasi yang akan dienkripsi adalah sinyal audio dengan format *.WAV*.
2. Algoritma enkripsi yang digunakan adalah *Baker Map*.
3. Lama waktu komputasi linier yang diujikan adalah 2 detik, 4 detik, 6 detik, 8 detik, 10 detik dan 12 detik.
4. Lama waktu komputasi geometri yang diujikan adalah 2 detik, 4 detik, 16 detik, 32 detik dan 64 detik.
5. Proses dari Algoritma Baker Map hanya menggunakan ukuran matrik 256 x 256, matrik 512 x 512 dan matrik 1024 x 1024.
6. Proses enkripsi menggunakan variasi kunci 2, 8, 16, 32, 64, dan acak.

7. Tidak memperhatikan proses pentransmisiannya dan diasumsikan tidak ada error pada saat transmisi data.
8. Simulasi dilakukan dengan menggunakan *software Matlab* 7.4.0.287 (R2007a).

1.5 Metodologi Penelitian

Metodologi penelitian yang digunakan dalam pencapaian Tugas Akhir ini adalah :

1. Studi Literatur yang dilakukan untuk mempelajari konsep dasar dan teori pendukung yang berhubungan dengan permasalahan pada tugas akhir ini.
2. Pencarian data yang dilakukan sebagai bahan untuk proses analisa. Data yang digunakan adalah data berupa audio dengan *format .WAV*.
3. Merancang program simulasi pada software *Matlab* 7.4.0.287 (R2007a) yang akan digunakan untuk pengimplementasian proses enkripsi.
4. Menganalisa data yang telah didapat dengan program simulasi sesuai dengan parameter yang telah ditentukan.
5. Mengambil kesimpulan dari hasil analisa yang telah dilakukan dilihat dari parameter yang ada serta memberi saran untuk penelitian selanjutnya.

1.6 Sistematika Penulisan

BAB I Pendahuluan

Pada bab ini dijelaskan mengenai latar belakang, tujuan, rumusan masalah, batasan masalah, metodologi penelitian dan sistematika penulisan.

BAB II Dasar Teori

Pada bab ini berisikan mengenai teori dasar enkripsi, input sistem dan teori dasar mengenai metode *Baker Map* yang digunakan pada sistem dan skema dari metode tersebut.

BAB III Perancangan Dan Implementasi Enkripsi Dengan *Baker Map*

Pada bab ini berisikan rancangan sistem dan simulasi sistem enkripsi dengan masukan audio dengan *format .WAV* dan kemudian dienkripsi menggunakan software *Matlab* 7.4.0.287 (R2007a).

BAB IV Hasil Analisa Simulasi

Bab ini berisi hasil penelitian dari hasil simulasi, perbandingan tingkat efisiensi performansi dari sistem enkripsi dan analisis statistik dari keluaran enkripsi.

BAB V Penutup

Pada bab ini akan di muat kesimpulan akhir dari analisis yang telah dilakukan pada bab IV, dan saran yang berkaitan dengan masalah yang dibahas untuk pengembangan penelitian ini.

BAB V

KESIMPULAN DAN SARAN

5.1. Kesimpulan

Dari pengujian dan analisis sistem yang telah dilakukan, maka dapat diambil kesimpulan sebagai berikut :

1. Telah berhasil didesain dan disimulasikan sistem enkripsi audio dengan menggunakan algoritma *Baker Map*.
2. Waktu proses enkripsi dari algoritma *Baker Map* dipengaruhi oleh ukuran matrik dan jumlah iterasi. Hubungan matrik dan jumlah iterasi dengan waktu proses adalah linier dengan gradien 0,067.
3. Waktu proses dekripsi dari algoritma *Baker Map* dipengaruhi oleh ukuran matrik dan jumlah iterasi. Hubungan matrik dan jumlah iterasi dengan waktu proses adalah linier dengan gradien 0,253.
4. Untuk ukuran matrik MxM (256, 512, dan 1024), enkripsi dengan *Baker Map* masing-masing membutuhkan waktu 1.04 detik, 23.19 detik dan 185.81 detik.
5. Proses enkripsi dan dekripsi dengan menggunakan variasi kunci acak memiliki waktu proses 6,67% lebih cepat dibandingkan dengan menggunakan variasi kunci konstan.
6. Tingkat keamanan dilihat dari ketahanan terhadap *brute force attack* untuk metode enkripsi *Baker Map* dengan nilai yang diperoleh yaitu 1,66 x 10^{55} tahun sedangkan untuk metode enkripsi *DES* dengan nilai yang diperoleh yaitu 9,94 x 10^{11} tahun, maka dapat dinyatakan enkripsi dengan algoritma *Baker Map* ini aman.
7. Untuk ukuran matrik MxM (256, 512, dan 1024), enkripsi dengan *DES* masing-masing membutuhkan waktu 3.39 detik, 205.98 detik dan 3290.96 detik sehingga dapat dinyatakan enkripsi dengan algoritma *Baker Map* memiliki waktu proses lebih cepat dibandingkan metode *DES*.

5.2. Saran

1. Digunakannya bahasa pemrograman yang lain seperti C++ untuk mengimplimentasikan sistem enkripsi ini dengan waktu proses yang lebih baik, terutama pada matrik berukuran besar.
2. Mengkombinasikan algoritma *Baker Map* dengan algoritma enkripsi lainnya untuk mendapatkan hasil yang lebih optimal, baik dilihat dari lamanya proses enkripsi ataupun dilihat dari ketahanannya terhadap *brute force attack*.

DAFTAR PUSTAKA

[1] Adriansyah, Rizky. 2009. Implementasi Enkripsi Sebagian Frame Video Dengan Menggunakan Metode Gabungan Advanced Encryption Standard (AES) Dan Baker Map. Bandung : Institut Teknologi Telkom.

[2] Andayani, Nurina. 2009. Desain dan Implementasi Enkripsi Pada Sebagian Frame Video Menggunakan Metode Baker Map dan SDES. Bandung : Institut Teknologi Telkom.

[3] Bishnu S. Atal, Vladimir Cuperman, and Geisha A., 1993. Speech and Audio Coding for Wireless and Network Application. Kluwer academic publisher: Boston/Dordrecth/London.

[4] Hafsahtiarni, Rifa. 2009. Desain dan Implementasi Metode Gabungan Cat Map dan Baker Map Untuk Peningkatan Sekuritas Pada Enkripsi Citra Digital. Bandung : Institut Teknologi Telkom.

[5] J. Fridrich, Symmetric Ciphers Based on Two-Dimensional Chaotic Maps, International Journal of Bifurcation and Chaos (IJBC) in Applied Sciences and Engineering, Vol. 8, No.6, (1998), 1259-1284.

[6] J. Fridrich.1997. Image Encryption Based on Chaotic Maps.

[7] Munir, Rinaldi. Matematika Diskrit. Bandung.

[8] Susanto, Iskan. 2009. Analisa Dan Implementasi Enkripsi-Dekripsi Suara Menggunakan Algoritma Rijndael. Diktat Kuliah. Bandung : Institut Teknologi Telkom.

[9] Tritoasmoro, Iwut, Iwan, ST. MT, Multimedia Signal Processing, Diktat Kuliah. Program Studi Teknik Telekomunikasi. Bandung : Institut Teknologi Telkom.

[10] Tritoasmoro, Iwut, Iwan, ST. MT, Analisa Wavelet, Diktat Kuliah. Program Studi Teknik Telekomunikasi. Bandung : Institut Teknologi Telkom.

[11] Tritoasmoro, Iwut, Iwan, ST. MT, Sinyal Dalam Domain Digital, Diktat Kuliah. Program Studi Teknik Telekomunikasi. Bandung : Institut Teknologi Telkom.

[12] http://www.buletindo.com/pengenalankriptografi

[13] http://www.buletindo.com/enkripsi-file-text-dengan-algoritma-caesar-chiper, diakses tanggal 5 April 2009.

[14] http://www.google.com/multimedia

[15] http://www.google.com/pembuatanperangkatlunakwavemanipulatoruntukmemanipulasifilewav

[16] http://www.google.com/pengolahan-sinyal-digital diakses tanggal 20 Juli 2010.

[17] http://www.wikipedia.com/nyquist-shannon-sampling-theorem