

# UNIVERSITAS BINA NUSANTARA

---

Jurusan Teknik Informatika  
Skripsi Sarjana Komputer  
Semester Ganjil tahun 2005/2006

## PERANCANGAN SISTEM PROTEKSI FILE DENGAN PASSWORD SUARA

**Rendy Sesario 0600615431**  
**Samanta Limbrada 0600623635**

### Abstrak

Perancangan sistem proteksi file dengan password suara pada penelitian ini dilakukan untuk menciptakan suatu aplikasi enkripsi file yang lebih aman dibandingkan dengan aplikasi enkripsi standar yang hanya memerlukan password berupa karakter. Solusi yang dipilih yaitu dengan penggunaan *speaker verification* sebagai pengganti *password*. Dengan kata lain, untuk membuka proteksi, user perlu mengucapkan passwordnya. Metode penelitian yang dipakai yaitu studi pustaka dan analisis mengenai algoritma enkripsi dan metode pengenalan suara yang paling baik. Hasilnya merupakan sebuah aplikasi enkripsi file dengan *password* suara yang menggunakan algoritma enkripsi Blowfish, dan menggunakan metode *Mel-frequency Cepstrum Coefficients* (MFCC) dan *Vector Quantization* sebagai metode untuk melakukan pengenalan pembicara (*speaker verification*). Setelah penelitian selesai, dapat disimpulkan bahwa enkripsi Blowfish termasuk algoritma enkripsi yang paling aman saat ini, dan MFCC – *Vector Quantization* (dengan *VQ-distortion* antara 2 sampai 3) merupakan metode pengenalan pembicara yang cukup baik, walaupun masih memerlukan lingkungan yang tidak bising dalam perekaman suara, dan cara pengucapan/intonasi yang tidak berubah.

### Kata Kunci

Pengenalan suara, *speaker verification*, enkripsi Blowfish, *Mel-frequency Cepstrum Coefficients*, *Vector Quantization*

## PRAKATA

Puji syukur kepada Tuhan Yang Maha Esa karena berkat rahmat-Nya penulis dapat menyelesaikan skripsi ini. Skripsi ini disusun untuk memenuhi syarat penyelesaian studi program sarjana di Fakultas Teknik Komputer Jurusan Teknik Informatika Universitas Bina Nusantara Jakarta.

Pada penulisan skripsi ini, penulis memilih bidang *artificial intelligence* dengan topik yang berjudul “Perancangan Sistem Proteksi File Dengan Password Suara”.

Penyusunan dan penulisan skripsi ini adalah suatu proses yang panjang dan tidak lepas dari bantuan, bimbingan dan dukungan berbagai pihak. Untuk itu pada kesempatan ini penulis ingin memberikan apresiasi, penghormatan dan rasa terima kasih yang sebesar-besarnya kepada Bapak Haryono Soeparno, Ir., M.Sc., Dr. selaku pembimbing skripsi yang telah bersedia meluangkan waktunya untuk memberikan bimbingan dan membagikan ilmu yang sangat bermanfaat kepada penulis sehingga skripsi ini dapat diselesaikan.

Ucapan terima kasih juga penulis sampaikan kepada :

1. Prof. Gerardus Polla, DR., Drs, M.App.Sc selaku Rektor Universitas Bina Nusantara, yang telah memberi kepercayaan dan kesempatan kepada penulis untuk mengikuti kuliah dan menyelesaikan skripsi.
2. Bapak H.M. Subekti, BE, M.Sc selaku Kepala Jurusan yang telah menyetujui pembuatan skripsi ini.
3. Orang tua dan keluarga kami yang telah memberikan dukungan penuh bagi kami sehingga kami dapat menyelesaikan penulisan skripsi ini dengan baik.

4. Rekan-rekan mahasiswa Bina Nusantara peminatan *Artificial Intelligence* angkatan 2002 yang memberikan bantuan, saran dan kritik dan dorongan yang sangat berarti kepada penulis.
5. Semua pihak yang telah terlibat dalam penulisan skripsi dan tidak dapat disebutkan satu persatu, yang telah membantu penulis sehingga dapat terselesaikannya penulisan skripsi ini.

Akhir kata Semoga Allah yang Maha Pengasih dan Maha Penyayang melimpahkan berkat, rahmat, dan karuniaNya kepada kita semua.

# DAFTAR ISI

Halaman Judul Luar	
Halaman Judul Dalam	
Halaman Persetujuan Hard Cover.....	iii
Halaman Pernyataan Dewan Penguji .....	iv
Abstrak .....	vi
Prakata .....	vii
Daftar Isi .....	ix
Daftar Tabel .....	xiv
Daftar Gambar .....	xv
Daftar Lampiran .....	xvii

## **Bab 1 Pendahuluan**

1.1	Latar Belakang .....	1
1.2	Ruang Lingkup .....	2
1.3	Tujuan dan Manfaat .....	3
1.4	Metodologi.....	3
1.5	Sistematika Penulisan .....	4

## **Bab 2 Landasan Teori**

2.1	Kriptografi .....	6
2.1.1	Sejarah Singkat .....	7

2.1.2	Symmetric dan Symmetric Cryptosystem .....	7
2.1.3	Serangan <i>Cryptanalyst</i> .....	8
2.1.4	<i>Password</i> dan Jenis Kunci Enkripsi Lainnya .....	9
2.1.5	Penggunaan Enkripsi .....	10
2.2	Teknik Enkripsi <i>Blowfish</i> .....	11
2.2.1	Latar Belakang .....	11
2.2.2	Algoritma Blowfish .....	12
2.3	Sejarah Pengenalan Suara .....	16
2.4	Sinyal Analog .....	18
2.5	Sinyal Digital .....	20
2.6	<i>Speaker Recognition</i> (Pengenalan Pembicara) .....	20
2.6.1	Prinsip <i>Speaker Recognition</i> .....	21
2.6.2	Ekstraksi Ciri ( <i>Feature Extraction</i> ) Suara .....	23
2.6.3	Prosesor <i>Mel-frequency Cepstrum Coefficients</i> (MFCC) ...	24
2.6.4	<i>Vector Quantization</i> .....	30
2.6.5	<i>Pairwise Euclidean Distance</i> .....	31
2.6.6	Faktor yang Mempengaruhi Akurasi Verifikasi Pembicara..	32

### **Bab 3 Perancangan Sistem**

3.1	Gambaran Umum Sistem .....	34
3.2	Proses Enkripsi .....	35
3.2.1	Pemilihan File .....	35
3.2.2	Perekaman Suara .....	36
3.2.3	<i>Feature Extraction</i> .....	36

3.2.4	Penyimpanan Vektor Suara .....	37
3.2.5	Enkripsi Blowfish .....	37
3.2.6	Penyimpanan File Hasil Enkripsi .....	37
3.3	Proses Dekripsi .....	38
3.3.1	Pemilihan File .....	38
3.3.2	Perekaman Suara .....	38
3.3.3	Feature Extraction .....	39
3.3.4	Perhitungan <i>Euclidean Distance</i> .....	39
3.3.5	Dekripsi <i>Blowfish</i> .....	40
3.3.6	Penyimpanan Hasil Dekripsi .....	40
3.4	Rancangan Layar .....	40
3.4.1	Rancangan Layar Utama .....	41
3.4.2	Rancangan Layar Informasi .....	41
3.4.3	Perancangan Layar Enkripsi .....	42
3.4.4	Rancangan Layar Dekripsi .....	43
3.5	<i>State Transition Diagram</i> .....	44
3.6	Spesifikasi Modul .....	46
3.6.1	Modul Enkripsi Blowfish .....	47
3.6.2	Modul Enkripsi Byte .....	47
3.6.3	Modul Dekripsi Blowfish .....	48
3.6.4	Modul Dekripsi Byte .....	49
3.6.5	Modul Proses Signal .....	49
3.6.6	Modul Verifikasi .....	50
3.6.7	Modul MFCC .....	50

3.6.8	Modul Vector Quantization .....	51
3.6.9	Modul Euclidean Distance .....	52
3.6.10	Modul Main Program .....	53
3.6.11	Modul Form Enkripsi .....	53
3.6.12	Modul Form Dekripsi .....	54

## **Bab 4 Implementasi dan Evaluasi**

4.1	Spesifikasi Hardware dan Software yang digunakan dalam penelitian.....	56
4.2	Implementasi Aplikasi .....	56
4.3	Tampilan Layar .....	57
4.3.1	Tampilan Layar Menu Utama .....	57
4.3.2	Tampilan Layar Informasi .....	58
4.3.3	Tampilan Layar Enkripsi .....	59
4.3.4	Tampilan Layar Dekripsi .....	61
4.4	Evaluasi Hasil Penelitian .....	63
4.4.1	Percobaan dengan Menggunakan <i>Password</i> Berbeda pada User yang Sama .....	64
4.4.2	Percobaan dengan Menggunakan <i>Password</i> Sama pada User yang Berbeda .....	66
4.4.3	Percobaan dengan Menggunakan Berbagai Macam <i>Password</i> .....	68
4.4.4	Percobaan dengan Menggunakan <i>Password</i> yang Sama pada User yang Berbeda .....	69

4.4.5 Percobaan dengan Menggunakan Berbagai Macam Password .....	71
4.4.6 Percobaan dengan Sistem yang Berbeda .....	72

**Bab 5 Kesimpulan dan Saran**

5.1 Kesimpulan .....	73
5.2 Saran .....	74
<b>Daftar Pustaka</b> .....	76
<b>Riwayat Hidup</b> .....	77
<b>Lampiran</b>	



## DAFTAR TABEL

Tabel 4.1 Percobaan dengan <i>Password</i> yang Sama dari <i>User</i> yang Sama .....	64
Tabel 4.2 Percobaan dengan <i>Password</i> yang Hampir Sama dari <i>User</i> yang Sama .	64
Tabel 4.3 Percobaan dengan <i>Password</i> yang Sama dari <i>User</i> yang Sama .....	65
Tabel 4.4 Percobaan dengan <i>Password</i> yang Hampir Sama dari <i>User</i> yang Sama ..	65
Tabel 4.5 Percobaan dengan Menggunakan <i>Password</i> yang Sama dengan Urutan Suku Kata yang Tidak Terlalu Berbeda dari <i>User</i> yang Sama .....	67
Tabel 4.6 Percobaan dengan Menggunakan <i>Password</i> yang Sama dengan Urutan Suku Kata yang Tidak Terlalu Berbeda dari <i>User</i> yang Sama .....	67
Tabel 4.7 Percobaan dengan Menggunakan <i>Password</i> yang Sama dengan Urutan Suku Kata Acak dari <i>User</i> yang Sama .....	68
Tabel 4.8 Percobaan dengan Menggunakan <i>Password</i> yang Sama dengan Urutan Suku Kata Acak dari <i>User</i> yang Sama .....	69
Tabel 4.9 Percobaan dengan <i>Password</i> yang Sama dari <i>User</i> yang Berbeda .....	70
Tabel 4.10 Percobaan dengan <i>Password</i> yang Sama dari <i>User</i> yang Berbeda .....	70
Tabel 4.11 Percobaan dengan Berbagai Macam <i>Password</i> .....	71
Tabel 4.12 Percobaan dengan Sistem yang Berbeda .....	72

## DAFTAR GAMBAR

Gambar 2.1 Algoritma Enkripsi Blowfish .....	14
Gambar 2.2 Fungsi F dalam Algoritma Enkripsi Blowfish .....	15
Gambar 2.3 Sinyal Analog Diubah Menjadi Sinyal Digital .....	20
Gambar 2.4 <i>Speaker Verification</i> .....	21
Gambar 2.5 <i>Speaker Identification</i> .....	22
Gambar 2.6 Input Suara .....	24
Gambar 2.7 Prosesor <i>Mel-frequency Cepstrum Coefficients</i> .....	24
Gambar 2.8 Input Suara Setelah Melalui Tahap <i>Frame Blocking</i> .....	25
Gambar 2.9 Input Suara Setelah Melalui FFT .....	27
Gambar 2.10 Input Suara Setelah Melalui Tahap <i>Mel-frequency Wrapping</i> .....	28
Gambar 2.11 Input Suara Setelah Melalui Tahap <i>Cepstrum</i> .....	29
Gambar 3.1 Skema Sistem .....	34
Gambar 3.2 Hierarki Layar .....	40
Gambar 3.3 Rancangan Layar Utama .....	41
Gambar 3.4 Rancangan Layar Informasi .....	42
Gambar 3.5 Perancangan Layar Enkripsi .....	43
Gambar 3.6 Perancangan Layar Dekripsi .....	43
Gambar 3.7 <i>State Transition Diagram</i> pada Proses Enkripsi .....	45
Gambar 3.8 <i>State Transition Diagram</i> pada Proses Dekripsi .....	46
Gambar 4.1 Tampilan Layar Menu Utama .....	58
Gambar 4.2 Tampilan Layar Informasi .....	58
Gambar 4.3 Tampilan Layar Enkripsi .....	59

Gambar 4.4 Tampilan Layar Enkripsi dengan Pesan Kesalahan .....	59
Gambar 4.5 Tampilan Layar Enkripsi dengan Pesan Kesalahan .....	60
Gambar 4.6 Tampilan Layar Enkripsi dengan Pesan Berhasil .....	60
Gambar 4.7 Tampilan Layar Dekripsi .....	61
Gambar 4.8 Tampilan Layar Dekripsi dengan Pesan Kesalahan .....	61
Gambar 4.9 Tampilan Layar Dekripsi dengan Pesan Kesalahan .....	62
Gambar 4.10 Tampilan Layar Dekripsi dengan Pesan Berhasil .....	62
Gambar 4.11 Tampilan Layar Dekripsi dengan Pesan Gagal .....	63

# DAFTAR LAMPIRAN

Listing Program .....	L1
-----------------------	----