# GRAPHICAL PASSWORD AUTHENTICATION USING IMAGE SELECTION

**Wiwi Liguna[1], Agus Virgono[2], Iwan Iwut Tirtoasmoro[3]**

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

**Abstrak**
**-**

**Kata Kunci : -**

**Abstract**
**-**

**Keywords : -**

# BAB I
# PENDAHULUAN

## 1.1 Latar Belakang

*User authentication* merupakan komponen utama dalam infrastruktur keamanan akhir – akhir ini. *User authentication* juga merupakan masalah untuk setiap sistem akses layanan keamanan menjadi berharga, informasi aman, dan layanan *personality*. Ada 3 cara untuk menentukan *user authentication* : *knowledge-based system, token-based system,* dan *system based on biometrics*.

Pada saat ini skema *token-based* sangat umum digunakan seperti *key card*, *bank card*, dan *smart card*. Sebagai contoh digunakan untuk ATM (Anjungan Tunai Mandiri). *Biometrics system* memang lebih aman dibandingkan dengan kedua authentikasi lainnya tapi ada beberapa permasalahan pada sistem biometrics salah satunya harus menggunakan alat khusus yang dianjurkan, mahal dan mungkin penggunaanya lebih rumit.

*Textual password* pada umumnya menggunakan karakter alfanumerik (atau printable ASCII characters) untuk mengindentifikasi pengguna yang bersangkutan. *Password* yang sederhana memudahkan pengguna untuk mengingatnya tetapi mudah juga untuk dipecahkan. Sedangkan *password* yang rumit, penggunaannya tidak nyaman tapi sulit untuk dipecahkan. Bagaimanapun juga penggunaan *textual password* dapat dipecahkan cepat atau lambat, karena *user* berulang – ulang memilih *password* yang mudah dikenali. Hal ini disebabkan karena ingatan manusia yang terbatas. Kasus ini biasanya disebut *"small dictionary*".

Penyerangan terhadap "small dictionary" menurut Dr. Klein [Klein 1990] ini ternyata dapat berhasil dilakukan, sekitar 25% dari 14000 *password* dapat di pecahkan oleh sebuah "dictionary" hanya dengan 3 juta masukan (ukuran dictionary 21.5 bits).

Disisi lain, penggunaan alat – alat yang besifat *personal* dan mobilitas yang tinggi cenderung meningkat akhir – akhir ini. Ada beberapa masalah dalam hal *personality*: jika *user authentication* tidak diaktifkan, memungkinkan pengguna umum dapat memakainya. Sehingga ini bukan bersifat *personal* lagi.

Bahkan apabila *user authentication* ini diaktifkan, mungkin saja mekanismenya lemah. Sekali mengaktifkan authentikasi ini, harus berulang – ulang diperbaharui.

Dalam tugas akhir ini, saya akan membuat aplikasi menggunakan skema graphical *password* dengan menggunakan gambar sebagai node – node yang nantinya dapat dikombinasikan layaknya *password* pada umumnya. Dan diharapkan keamanan berbading lurus dengan kenyamanan.

## I.2. Perumusan Masalah

1. Metode *textual password* bisa dipecahkan (kekuatan *textual password*).
2. Gambar lebih mudah dikenali dibandingkan teks.
3. Tingkat keamanan dan kenyamanan penggunaan atuhentication.
4. Kesulitan mencari dan mengingat *password* yang ingin digunakan.
5. Parameter – parameter yang dianalisa :
   - Efektifitas, meliputi daya ingat seseorang tentang *picture/image* yang digunakan sebagai *password.*
   - Kecepatan Waktu Entry, waktu yang dibutuhkan seseorang saat meng*entry picture/image* sebagai *password*.
   - Kekuatan *password* secara umum.
   - User satisfaction (Kepuasan Pengguna), meliputi *Mean Opinion Square*.
6. Parameter – parameter yang disimpulkan :
   - Apakah Picture *Password* dapat dijadikan alternatif authentication yang cukup dapat diandalkan dibandingkan metode authenticatin pada umumnya.
   - Apakah Picture *Password* yang digunakan cukup dapat memenuhi kenyamanan yang diinginkan (MOS).

## I.3. Tujuan Pembahasan

Tujuan yang ingin dicapai dari penyusunan tugas akhir ini adalah:

1. Merancang Graphical *Password* menggunakan image selection (picture *password*).

2. Menganalisa performansi dari skema *password* tersebut meliputi parameter diatas.

## I.4. Batasan Masalah

Dalam pembangunan aplikasi ini dibatasi beberapa hal yaitu :

1. Panjang *password* maksimum yang digunakan 7 digit.
2. Menggunakan pengamanan kriptografi hash MD5.
3. Gambar sudah ada (ditentukan dari awal) jadi pengguna hanya memilih.
4. Setiap gambar berbentuk persegi dengan ukuran 80x80 piksel.
5. Digunakan untuk pengguna tunggal (*single user*) dan *single password*.
6. Gambar sebagai interface inputan.
7. Sistem tidak melakukan proses pengkodean gambar.
8. File penyimpanan berekstensi Reg (.reg).
9. Sistem diterapkan dan hanya berjalan pada Sistem Operasi Windows.

## I.5. Metodologi Penyelesaian Masalah

Dalam penelitian nantinya, penulis akan melakukan metode sebagai berikut :

1. Studi literatur.
   - Mengambil referensi – referensi yang menunjang penelitian tugas akhir ini.
   - Pengumpulan data dari penelitian sebelumnya tentang skema *Graphical password*.
2. Perancangan.
   - Merancang aplikasi *picture password* yang akan digunakan.
3. Percobaan.
4. Validasi
5. Analisa.
   - Menganalisa parameter – parameter tersebut di atas dengan analisa teknis dan penilaian berdasarkan MOS.
6. Kesimpulan dan Saran.

## I.6. Sistematika Penulisan

**BAB I PENDAHULUAN**

Berisi latar belakang, perumusan masalah, batasan masalah, tujuan pembahasan, metodologi penyelesaian masalah dan sistematika penulisan.

**BAB II LANDASAN TEORI**

Berisi penjelasan umum tentang landasan teori yang berkaitan dengan penyusunan tugas akhir.

**BAB III PERANCANGAN DAN DESAIN SISTEM**

Berisi analisis sistem yang akan dikembangkan mencakup analisa kebutuhan sistem, perancangan dan desain sistem, sehingga dapat dipahami dengan mudah.

**BAB IV IMPLEMENTASI DAN ANALISIS PROGRAM**

Membahas analisa hasil percobaan berdsarkan parameter yang telah disebutkan di atas.

**BAB V KESIMPULAN DAN SARAN**

Diuraikan kesimpulan dan saran yang didapat dari hasil pengembangan sistem.

Telkom University

# BAB V
# KESIMPULAN DAN SARAN

## 5.1 Kesimpulan

Beberapa kesimpulan yang dapat diambil adalah sebagai berikut :

1. Metode sistem ini dapat digunakan untuk alat – alat yang menggunakan *stylus* seperti PDA, dsb.
2. Hanya ditemukan dua jenis kesalahan pada *picture password* diantaranya *errorneous selection* 6% dan *errorneous code* 3%.
3. Waktu rata – rata yang dibutuhkan dalam meng*entry* kata kunci sekitar 2.5 detik untuk setiap *layer*nya dan total waktu rata – rata sebesar 18 detik.
4. Kekuatan dari *picture password* apabila di*brute force* secara manual dibutuhkan waktu sekitar 118.73 tahun.
5. Menurut percobaan didapati 94% responden yang puas dengan program *Picture password.*

## 5.2 Saran

Beberapa saran untuk pengembangan sistem selanjutnya adalah sebagai berikut :

1. Pengguna dapat menentukan tema gambar yang sesuai dengan karakternya masing – masing.
2. Sistem dapat diimplementasikan langsung pada PDA.
3. Letak *file* hasil dari proses *create password* mungkin tersebar sehingga lebih aman.
4. Sistem dapat dikembangkan untuk *multi user* dan *multi password* apabila alat yang dipilih bukan PDA
5. Apabila diterapkan pada PDA maka digunakan bahasa pemrograman C++ dengan struktur pemprograman yang lebih baik, sehingga waktu pemrosesan jauh lebih efektif.
6. Digunakan file terpisah dalam format dll sebagai *database* dari gambar tersebut, sehingga ukuran file menjadi lebih kecil.

Keuntungan lainnya yaitu gambar juga bisa di*update* oleh pengguna.

# DAFTAR PUSTAKA

1. Pranata, Anthony. 2000. "Pemrograman Borland Delphi edisi 3", Andy Yogyakarta.
2. Suo, Xiaoyuan. 2006. "A Design and Analysis of Graphical Password", Georgia State University.
3. Wayne Jansen, Serban Gavrila, Vlad Korolev, Rick Ayers, Ryan Swanstrom. 2003, "Picture Password: A Visual Login Technique for Mobile Device". USA
4. Tao, Hai. 2006. "Pass-Go, a New Graphical Password Scheme", Canada.
5. Mulyana, Marta, Hendra. 1998. "Perancangan Rangkaian Digital MD5 Untuk Tanda Tangan Digital". Bandung, STT Telkom.
6. Fadli, Ilham. 1998. "Pembangunan Sistem Keamanan Akses Komputer Berdasarkan Pola Pendekatan Papan Kunci". Bandung, STT Telkom.
7. Website Delphi. www.delphi-id.org
8. PicturePassword-Security Software for Palm and Pocket PC Feature, 2004. www.Softava.com
9. Pass-throughts: Authentication With Your Mind, 2005. eprint.iacr.org/2005/121.html
10. Patrick, Andrew. 2002, "Human Factor of Security Systems: A Brief Review". Canada.
11. KLEIN, D. 1990. Foiling the cracker: A survey of, and improvements to, password security. In Proceedings of the 2nd USENIX Security Workshop. 5-14.
12. [RFC1321] Ronald L. Rivest, The MD5 Message-Digest Algorithm, RFC 1321, April 1992