

DETEKSI KEDIPAN MATA DENGAN HAAR CASCADE CLASSIFIER DAN CONTOUR UNTUK PASSWORD LOGIN SISTEM

Muhammad Syarif¹, Wijanarto²

^{1,2}Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro Semarang
Jl. Nakula I, No. 5-11, Semarang, Kode Pos 50131, Telp. (024) 3515261, 3520165 Fax: 3569684
E-mail : muhammad.syarif12@gmail.com¹, wijanarto.dinus@gmail.com²

Abstrak

Keamanan merupakan menjadi prioritas utama dalam era teknologi informasi, yang meliputi keamanan data, hardware atau software. Untuk menjaga keamanan diperlukan data pribadi sebagai autentifikasi dan validasi pengguna yang sah. Password merupakan data pribadi yang dimasukan pengguna secara langsung melalui keyboard. Memasukan data password melalui keyboard mudah dicuri dengan aplikasi Keylogger. Tahun 2008, 78% terdapat ancaman pencurian informasi rahasia data pengguna, dan 76% menggunakan komponen keystroke logging untuk mencuri informasi seperti akun bank online. beberapa variasi password yang dapat meminimalisir interaksi langsung pengguna dengan keyboard adalah memanfaatkan kedipan mata menjadi password. Dalam paper ini akan di pakai teknik Haar Cascade Classifier sebagai metode deteksi bagian tubuh tertentu suatu obyek, dan metode Contour sebagai deteksi kontur pada object spesifik, teknik ini dapat mendeteksi mata dan indikasi adanya kedipan, berdasarkan jarak, posisi obyek dan posisi sumber cahaya tertentu. Hasil dari penelitian yang di lakukan dengan memanfaatkan template deteksi kontur mata sempurna sebagai acuan kedipan mata. Nilai threshold juga berpengaruh pada hasil kontur yang dihasilkan dari berbagai jenis mata baik bentuk maupun warnanya. Berdasarkan hasil pengujian terhadap 15 sampel password kedipan, didapatkan akurasi 71,43 %, dan pengujian keystroke dengan aplikasi keylogger, password kedipan tidak terekam dalam log file keylogger.

Kata Kunci: Deteksi kedipan mata, Haar cascade Classifier, Contour, password, login sistem.

Abstract

Security is a top priority in the era of information technology, which includes data security, hardware or software. It is necessary to maintain the security of personal data as authentication and validation of legitimate users. Passwords are personal data that the user entered directly via the keyboard. Entering the password data via Keyboard easily stolen by the keylogger applications. In 2008, 78% contained the threat of theft of confidential information about the user data, and 76% using keystroke logging component to steal information such as online bank account. Several variations of passwords that can minimize direct interaction with the user is utilizing a wink keyboard into a password. In this paper will be used Haar Cascade Classifier method as detection of particular body part of an object, and methods of Contour as the detection of the contour for the object-specific, this technique can detect eye and blink indication, based on the distance, the position of the object and the position of the light source specified. Results of the study done by utilizing the perfect eye contour detection template as a reference blink of an eye. Threshold value also affects the results of contours generated from various types of eye shape or color. Based on the test results of 15 samples flicker password, obtained 71.43% accuracy, and testing the application keystroke keylogger, password flicker is not recorded in the log file keylogger.

Keywords: Detection of the blink of an eye, Haar Classifier cascade, Contour, password, login system.

1. PENDAHULUAN

Di dalam perkembangan teknologi, keamanan menjadi salah satu prioritas utama. Baik keamanan data, software, ataupun hardware yang bertujuan menghindari hal yang tidak diinginkan. Dalam hal keamanan dibutuhkan data pribadi tertentu sebagai autentikasi atau validasi pengguna yang sah. Salah satu contoh bentuk autentikasi yang sering digunakan adalah user id dan password, dimana user id adalah pernyataan tentang siapa yang sedang mengakses dan password sebagai pembuktian bahwa orang tersebut benar adanya [1]. Dalam kedua bagian data autentikasi tersebut, yang menjadi perhatian utama adalah password.

Password dalam kamus dapat diartikan kata [2] rahasia atau frase yang hanya diketahui kelompok terbatas. Berdasarkan pembentukan katanya, password (p s'wûrd') yang diuraikan sebagai kata pass dan word adalah kata (word) yang diberikan sebelum seseorang diizinkan untuk lewat (pass). Password adalah suatu bentuk dari data autentikasi yang digunakan untuk mengontrol akses ke suatu sumber informasi [3]. Dalam bidang komputer password adalah deretan karakter yang diinputkan untuk mendapatkan akses terhadap file, aplikasi atau sistem komputer [4].

Walaupun disebut password, namun tidak selalu berbentuk susunan kata-kata dan angka yang memiliki arti, misalnya berupa paduan huruf, angka dan kode yang tidak memiliki arti sehingga sulit untuk ditebak [3]. Umumnya pengguna akan memasukkan dengan cara mengetikkan password ke form yang telah disediakan. Namun hal ini sangat beresiko atau rentan terhadap pencurian password tersebut. Salah satu contoh

adalah pencurian password menggunakan aplikasi Keylogger. Keylogger adalah aplikasi pengawasan perangkat lunak atau perangkat keras yang memiliki kemampuan untuk merekam setiap keystroke pengguna yang kemudian dibuat dalam sebuah log file. Aplikasi Keylogger dapat merekam informasi yang diketik setiap saat melalui keyboard [5]. Pada tahun 2008, 78% terdapat ancaman pencurian informasi rahasia data pengguna, dan 76% menggunakan komponen keystroke logging untuk mencuri informasi seperti akun bank online. [6]

Sebagai solusi mengatasi pencurian password melalui perekaman keystroke keyboard, dalam perkembangannya kini dapat dijumpai berbagai variasi metode memasukkan password, seperti slide (penggeseran), pattern (pola), face unlock atau face detection (deteksi wajah), voice detection (deteksi suara), finger print (deteksi sidik jari), dll. Beberapa bentuk metode tersebut bertujuan untuk mengurangi resiko mudahnya pencurian yang apabila pengguna mengetik password secara langsung otomatis password tersebut sudah diketahui dengan pemanfaatan keystroke. Bahkan untuk deteksi wajah, suara dan sidik jari tersebut sudah tidak menggunakan keyboard sebagai alat inputan password, yang tentu sudah pasti menghindari pencurian password melalui keystroke.

Dalam beberapa tahun terakhir, telah ada upaya untuk meningkatkan interface antara manusia dan komputer yang masih tradisional seperti keyboard dan mouse dengan interface yang cerdas yang memungkinkan pengguna untuk berinteraksi dengan komputer secara alami dan efektif. Tujuannya adalah mengembangkan komputer yang tanggap terhadap komunikasi secara

alami [7]. Salah satunya adalah menggunakan deteksi kedipan mata yang juga dapat dimanfaatkan sebagai media interaksi antara manusia dan komputer.

Deteksi kedipan mata yang dapat menjadi alat inputan alternatif, tentunya dapat pula dikembangkan untuk menjadi password pengguna untuk masuk ke dalam sistem. Seperti halnya deteksi wajah, deteksi sidik jari, deteksi retina, dan deteksi suara, deteksi kedipan mata ini tidak menggunakan interaksi keyboard lagi untuk memasukkan password. Dalam penelitian ini digunakan Haar Cascade Classifier sebagai pendeteksi bagian tubuh, khususnya wajah dan mata, serta menggunakan Contour sebagai metode untuk mendeteksi kedipan mata.

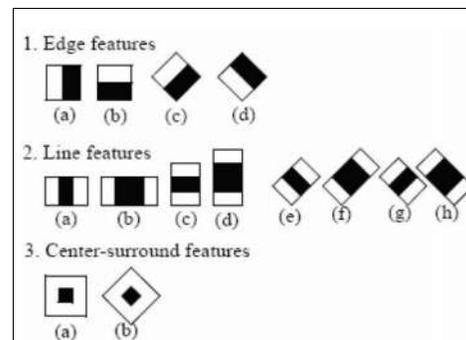
Maka perlu dilakukan penelitian yang berjudul “Implementasi Deteksi Kedipan Mata dengan Haar Cascade Classifier dan Contour Sebagai Password Login Sistem”. Dengan penelitian ini diharapkan dapat menjadikan deteksi kedipan mata sebagai metode password baru untuk masuk ke sistem, yang tidak lagi menggunakan keyboard sebagai alat inputan karena rentan dengan pencurian password melalui keystroke. Sekaligus ikut dalam mengembangkan peningkatan interface antara manusia dan komputer yang lebih natural.

2. METODE

2.1. Haar Cascade Classifier

Haar like feature atau yang dikenal sebagai Haar Cascade Classifier merupakan *rectangular* (persegi) *feature*, yang memberikan indikasi secara spesifik pada sebuah gambar atau *image*. Haar cascade classifier berasal

dari gagasan Paul Viola dan Michael Jhon, karena itu dinamakan metode Viola & Jhon. Ide dari *Haar like feature* adalah mengenali obyek berdasarkan nilai sederhana dari fitur tetapi bukan merupakan nilai piksel dari *image* obyek tersebut. Metode ini memiliki kelebihan yaitu komputasi yang sangat cepat, karena hanya tergantung pada jumlah piksel dalam persegi bukan setiap nilai piksel dari sebuah *image*. Metode ini merupakan metode yang menggunakan statistik model (*classifier*). Pendekatan untuk mendeteksi objek dalam gambar menggabungkan empat kunci utama yaitu Haar like feature, Integral Image, Adaboost learning dan Cascade Classifier [8].



Gambar 1. Haar Like Features

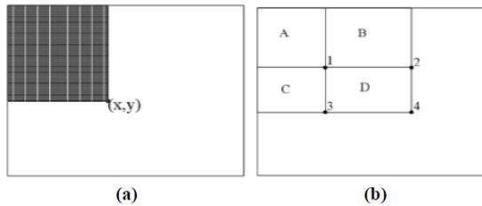
Haar Feature adalah fitur yang didasarkan pada Wavelet Haar. Wavelet Haar adalah gelombang tunggal bujur sangkar (satu interval tinggi dan satu interval rendah). Untuk dua dimensi, satu terang dan satu gelap. Selanjutnya kombinasi-kombinasi kotak yang digunakan untuk pendeteksian objek visual yang lebih baik. Setiap Haar-like feature terdiri dari gabungan kotak - kotak hitam dan putih.

$$f(x) = \text{SumBlack rectangle} - \text{SumWhite rectangle} \quad (1)$$

Adanya fitur Haar ditentukan dengan cara mengurangi rata-rata piksel pada

daerah gelap dari rata-rata piksel pada daerah terang. Jika nilai perbedaannya itu diatas nilai ambang atau *threshold*, maka dapat dikatakan bahwa fitur tersebut ada. Nilai dari Haar-like feature adalah perbedaan antara jumlah nilai-nilai piksel *gray level* dalam daerah kotak hitam dan daerah kotak putih. dimana untuk kotak pada Haar like feature dapat dihitung secara cepat menggunakan “*integral image*”.

Integral Image digunakan untuk menentukan ada atau tidaknya dari ratusan fitur Haar pada sebuah gambar dan pada skala yang berbeda secara efisien.



Gambar 2. Integral Image

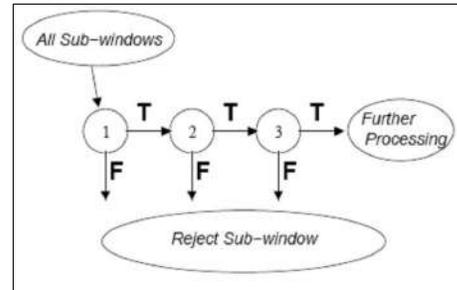
Seperti yang ditunjukkan oleh gambar di atas setelah pengintegrasian, nilai pada lokasi piksel (x,y) berisi jumlah dari semua piksel di dalam daerah segiempat dari kiri atas sampai pada lokasi (x,y) atau daerah yang diarsir. Guna mendapatkan nilai rata-rata piksel pada area segiempat (daerah yang diarsir) ini dapat dilakukan hanya dengan membagi nilai pada (x,y) oleh area segiempat.

$$ii(x,y) = \sum_{x'=0, y'=0}^{x,y} i(x',y') \tag{2}$$

dimana $ii(x,y)$ adalah integral image dan $i(x,y)$ adalah original image.

Sebuah metode untuk menggabungkan classifier yang

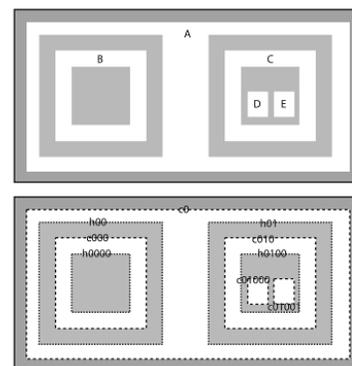
kompleks dalam sebuah struktur bertingkat yang dapat meningkatkan kecepatan pendeteksian obyek dengan memfokuskan pada daerah citra yang berpeluang saja. [8]



Gambar 3. Cascade Classifier

2.2. Contur

Contour adalah sebuah list yang berisi point yang dapat dikatakan mewakili dalam suatu curva dari sebuah gambar. Gambaran ini dapat berbeda-beda tergantung pada situasi yang dihadapi. Ada banyak cara untuk mewakili sebuah curva dalam suatu gambar. Contour digambarkan dalam OpenCV sebagai urutan (sequence) informasi yang dikodekan tentang lokasi dari point berikutnya dalam kurva. Fungsi yang ada pada OpenCV, menghitung contour dari gambar biner. Gambar biner dapat dihasilkan dari suatu threshold yang memiliki sudut yang implisit sebagai batas antara area yang positif dan negative.



Gambar 4. Contour pada OpenCV

Beberapa tahapan yang harus dilalui apabila ingin mendapatkan contour dari gambar RGB (true color). Tahapannya adalah :

- a) Membalikkan warna citra (negative color).
- b) Membuat gambar menjadi citra keabuan (gray scale).
- c) Thresholding dengan threshold binary Operasi thresholding dapat di hitung dengan

$$dst(x, y) = \begin{cases} maxVal, & \text{if } src(x, y) > thres \\ 0, & \text{otherwise} \end{cases} \quad (3)$$

- d) Menentukan contour dari gambar

2.4. Data Citra

Data citra yang dibutuhkan pertama adalah sampel data citra dari data real-time hasil webcam. Pengambilan data gambar dari webcam memiliki klasifikasi jarak antara objek dan webcam ± 40 – 60 cm, posisi kepala menghadap ke depan webcam, dan posisi sumber cahaya dari depan.

2.5. Deteksi Mata

Setelah mendapatkan data utama berupa sampel gambar hasil webcam, selanjutnya melakukan deteksi mata dengan haar cascade classifier. Hasil dari deteksi mata ditandai dengan kotak berwarna merah. Setelah mata dapat terdeteksi kemudian akan difokuskan pada area mata saja, untuk mendapatkan contour dari mata.



Gambar 5. Contoh Deteksi Mata dengan Haar Cascade Classifier

2.6. Menemukan Contour

Sebelum menemukan kontur, ada beberapa tahapan yang harus dilalui untuk mendapatkan kontur mata yang dapat terdeteksi sempurna. Tahapan-tahapannya adalah Negative color (membuat citra menjadi negative), merubah citra keabuan (grayscale), thresholding, dan menentukan contour.

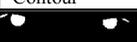
Tabel 1 : Proses sebelum mendapatkan contour

Sampel	Negative	Grayscale
		

Threshold mempengaruhi hasil penentuan kontur yang teridentifikasi mata atau tidak. Semakin kecil threshold maka akan banyak kontur ‘berukuran besar’ yang dihasilkan, bahkan membentuk satu kontur besar. Semakin besar threshold, maka semakin tidak terlihat kontur. Maka threshold haruslah tepat agar kontur mata sempurna.

Threshold dikatakan tepat apabila kontur yang dihasilkan memiliki suatu ukuran yang memungkinkan membentuk kontur mata sempurna, atau terdeteksi secara tepat pada area mata. Dalam penelitian ini, dengan jarak ± 40cm- 60cm, dengan hasil gambar webcam berukuran 640 x 482 piksel, maka kontur yang membentuk mata sempurna adalah kontur dengan tinggi 8 – 25 piksel. Kontur yang dibawah atau melebihi batas tersebut, akan dianggap bukan kontur mata.

Tabel 2 : Hasil Contour dengan Threshold tepat

Sample	Contour	TH	Hasil
		145- 225	

2.7. Deteksi Kedipan Mata

Kontur mata sempurna yang terdeteksi, maka dapat menjadi acuan untuk

mendeteksi kedipan mata. Apabila kontur pada area mata terdeteksi, mengindikasikan bahwa mata tersebut terbuka. Dan apabila kontur mata tidak ada (setelah sebelumnya terdeteksi) atau ukurannya terlalu kecil untuk membentuk kontur mata sempurna, dapat diindikasikan bahwa mata tersebut sedang tertutup.

Tabel 3 : Hasil deteksi kedipan mata

Mata	Kontour	Terdeteksi	Hsl
			R
			L
			P

2.8. Kedipan Sebagai Password

Hasil yang diperoleh dari deteksi kedipan mata akan mengirimkan data berupa karakter yang menjadi *password* masukan. Karakter tersebut terdiri dari ‘R’ sebagai kedipan kanan, ‘L’ sebagai kedipan kiri, dan ‘P’ sebagai kedipan kedua mata. Dalam penelitian ini panjang *password* ditentukan dengan panjang 6 karakter.



Gambar 6. Tampilan Prototype

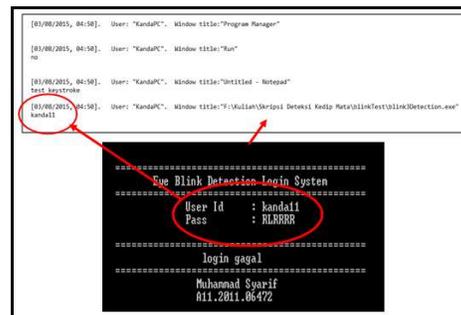
3. HASIL DAN PEMBAHASAN

Pengujian akan dilakukan terhadap metode yang diusulkan untuk mengetahui seberapa akurat deteksi mata, dan menguji apakah *password* terdeteksi secara *keystroke* atau tidak.

Tabel 4 : Pengujian akurasi kedipan

No	Kedipan Masukan	Kedipan Terdeteksi	Jml Ke dipan	Jumlah Kedipan Terdeteksi	Bnr	Slh
1	RRRRR R	RPRRLRPR R	6	9	6	3
2	LLLLL	LPPLPLL PRPPLPRP P	6	7	3	4
3	PPPPPP		6	9	6	3
4	RRRLL L	RRLPLL RRRLPLPP R	6	7	5	2
5	RRRPPP LLRR R		6	9	6	3
6		LLPRRRP	6	8	6	2
7	LLLPPP	LLPRRPRP	6	8	5	3
8	PPRRR	PLPPRRR	6	7	6	1
9	PPPLL	PPLLL	6	6	5	1
10	RLRLR L	RLRLPRL	6	7	6	1
11	RPRRP LRRL R	RPRRLRPR PRPRLP R	6	8	6	2
12		PRPRLP	6	7	3	4
13	LPLPLP	LPPLPLP	6	7	6	1
14	RLPPRL RRPLR P	RLPPRL RRLRPL	6	6	6	0
15		RRLRPL	6	7	5	2
Jumlah			90	112	80	32

Pengujian dilakukan menggunakan aplikasi keylogger, Family Keylogger v 2.71, untuk mendeteksi *password* kedipan mata. Hasil *keystroke* dapat diketahui dengan melihat *logfile* yang ada pada folder Family Keylogger.



Gambar 7. Hasil pengujian dengan Keylogger

Dari hasil pengujian dapat diperoleh nilai akurasi dan *error rate* dalam mendeteksi kedipan mata sebesar:

$$\text{akurasi} = \frac{80}{112} * 100\% = 71,43\%$$

$$\text{error rate} = \frac{32}{112} * 100\% = 28,57 \%$$

Dan pengujian dengan aplikasi Keylogger, password kedipan mata tidak terdeteksi.

4. KESIMPULAN DAN SARAN

4.1. Kesimpulan

Kesimpulan yang diperoleh dari penelitian ini adalah :

1. Implementasi dari metode Haar Cascade Classifier dan Contour dapat mendeteksi kedipan mata.
2. Metode Haar cascade classifier dapat mendeteksi bagian tubuh seperti wajah dan mata.
3. Dengan jarak, posisi obyek, dan posisi sumber cahaya tertentu dapat menghasilkan kontur mata sempurna sebagai acuan mendeteksi kedipan mata.
4. Selain jarak, posisi obyek dan posisi sumber cahaya, thresholding menjadi bagian penting untuk menghasilkan kontur yang sempurna.
5. Dengan threshold yang tepat, kontur beberapa jenis mata baik warna maupun bentuknya, dapat dikenali.
6. Dari uji coba dengan 15 jenis password kedipan, dengan total 112 kedipan yang di deteksi, berhasil mengenali 80 kedipan tepat sesuai kedipan dari obyek, dengan akurasi keberhasilan 71,43 %, dan error rate 28,57 %.

7. Pengujian menggunakan keylogger menunjukkan bahwa password dengan kedipan mata tidak terdeteksi, sehingga password tidak terekam dalam aplikasi keylogger.
8. Password dengan kedipan mata menghindari pencurian password secara keystroke.

4.2. Saran

Berikut merupakan beberapa saran yang perlu diperhatikan untuk pengembangan lebih lanjut dalam meningkatkan kualitas penelitian selanjutnya :

1. Dibutuhkan algoritma *Preprocessing* untuk mengoptimisasi data dari webcam, sehingga tanpa harus diambil dengan jarak, posisi obyek, dan posisi sumber cahaya tertentu.
2. Otomatisasi pemberian parameter threshold, agar dapat mengoptimalkan deteksi berbagai jenis mata baik bentuk atau warna mata.
3. Prototype sistem login dikembangkan agar memiliki database penyimpanan data user, karena masih tersimpan dalam variable.
4. Diharapkan kedepannya dikombinasikan dengan algoritma enkripsi untuk bagian user id, agar tidak tersimpan begitu saja dalam aplikasi perekam keystroke.
5. Dibutuhkan algoritma tambahan untuk tracking contour, sehingga dengan password sama namun mata bukan pemilik asli, maka pengguna tidak bisa masuk.

DAFTAR PUSTAKA

- [1] Sanusi, M. **The Genius Hacking Sang Pembobol Data**. Jakarta: Elex Media Komputido, 2010.

- [2] WEBDICTIONARY. CO. UK. webdictionary. co.uk. **webdictionary.co.uk**, 2015. Disponivel em: <<http://www.webdictionary.co.uk/definition.php?query=password>>. Acesso em: 12 maret 2015.
- [3] Sulianta, F. **Teknik Mengoptimalkan Password**. Jakarta: Elex Media Komputindo, 2009.
- [4] ENTERPRISE, J. **Teknik Mengamankan Password**. Jakarta: Elex Media Komputindo, 2010.
- [5] Newman, R. **Computing Security: Protecting Digital Resources**. Canada: Jones & Barlett Learning, 2009.
- [6] SYMANTEC. What the Latest Symantec Threat Report Means to SMBs. **Symantec**, 2015. Disponivel em: <http://www.symantec.com/solutions/article.jsp?aid=20090512_what_the_latest_symc_threat_report_means_to_smbs>. Acesso em: 06 Agustus 2015.
- [7] Grauman, K. et al. Communication Via Eye Blinks - Detection And Duration Analysis In Real Time. **IEEE**, 2001.
- [8] RD, K.; Pambudi, W. S.; Tomponu, A. N. Aplikasi Sensor Vision untuk Deteksi MultiFace dan Menghitung Jumlah Orang. **Seminar Nasional Teknologi Informasi & Komunikasi Terapan 2012 (Semantik 2012)**, Semarang, Juni 2012.