



PERANCANGAN PENGAMAN BRANKAS BERBASIS FACE RECOGNITION DENGAN METODE EIGENFACE YANG TERKONEKSI DENGAN HANDPHONE

Erfa Setiyoko

Article History:

Submitted: 25-07-2021
Revised: 13-08-2021
Accepted: 14 - 08 - 2021

Keywords:

Face Recognition, Eigenface, Raspberry Pi

Kata Kunci:

Face Recognition, Eigenface, Raspberry Pi

Koresponding:

Universitas Islam Kediri Kediri,
Jawa Timur, Indonesia
Email: erfa_setyo@yahoo.com

Abstract

In this era of pandemic, one of them is increasing significantly, one of which is theft, so the thing that encourages us to have storage devices for valuable items such as securities, jewelry, and money to avoid theft Safe is a tool or safe place that is usually used to store valuables. There are many types of safes on the market ranging from conventional to digital safes. Conventional safes that use manual combination codes have a low level of security. Biometric technology with facial recognition is an alternative to safe security problems with a higher level of security compared to conventional technology. Eigenface is a method used to transform and reduce the dimensions of an image by transforming it using eigenvalues and linear eigenvectors. The results showed that the level of accuracy of face detection using PCA (eigenface) can reach 95%, coupled with a security feature that is connected directly to the n

Abstrak

Di jaman pandemi seperti sekarang ini kasus kriminal meningkat secara signifikan salah satunya adalah pencurian, sehingga hal ini mendorong kita harus mempunyai adanya alat penyimpanan untuk barang-barang berharga seperti surat-surat berharga, perhiasan, dan uang agar terhindar dari pencurian. Brankas merupakan salah satu alat atau tempat aman yang biasa digunakan untuk menyimpan barang-barang berharga. Ada banyak jenis brankas yang ada di pasaran mulai dari brankas konvensional sampai digital. Brankas konvensional yang menggunakan kode kombinasi manual memiliki tingkat keamanan yang masih rendah. Teknologi *biometrik* dengan pengenalan wajah merupakan salah satu alternatif masalah keamanan brankas dengan tingkat keamanan lebih tinggi dibandingkan dengan teknologi konvensional. *Eigenface* merupakan suatu metode yang digunakan untuk mentransformasikan dan mereduksi dimensi dari suatu citra dengan mentransformasikannya menggunakan eigenvalue dan vektor *eigen* secara *linier*. Hasil penelitian didapatkan tingkat keakurasian deteksi wajah dengan menggunakan PCA (*eigenface*) dapat mencapai 95%, ditambah dengan fitur kemanan yang terhubung langsung kepada pemilik brankas menjadikan sistem ini memiliki tingkat keamanan yang cukup tinggi.

PENDAHULUAN

Teknologi komputer saat ini berkembang sangat pesat dan merupakan salah satu bidang yang mempunyai peranan sangat penting di beberapa aspek kehidupan manusia, termasuk pada bidang *security*. Di jaman pandemi seperti sekarang ini kasus kriminal meningkat secara signifikan salah satunya adalah pencurian, sehingga hal ini mendorong kita harus mempunyai adanya alat penyimpanan untuk barang-barang berharga seperti surat-surat berharga, perhiasan, dan uang agar terhindar dari pencurian. Brankas merupakan salah satu alat atau tempat aman yang biasa digunakan untuk menyimpan barang-barang berharga. Ada banyak jenis brankas yang ada di pasaran mulai dari brankas konvensional sampai digital. Brankas konvensional yang menggunakan kode kombinasi manual memiliki tingkat keamanan yang masih rendah. Teknologi biometrik dengan pengenalan wajah merupakan salah satu alternatif masalah keamanan brankas dengan tingkat keamanan lebih tinggi dibandingkan dengan teknologi konvensional. *Eigenface* merupakan suatu metode yang digunakan untuk mentransformasikan dan mereduksi dimensi dari suatu citra dengan mentransformasikannya menggunakan *eigenvalue* dan vektor *eigen* secara *linier*[1].

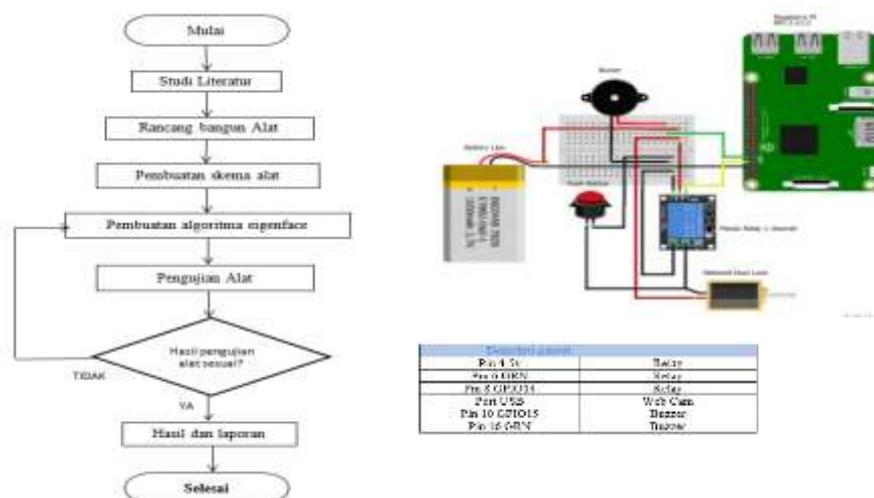
Kurniawan dan Zulus menggunakan metode *eigenface* dalam *smart home security* dengan *face recognition* menunjukkan hasil akurasi dengan rata-rata sebesar 72,5 %. Sistem berhasil melakukan pengenalan meskipun posisinya berbedabeda, karena yang digunakan adalah nilai dari *eigenface* tiap citra wajah yang dibandingkan [1]. Penelitian Septian dkk. tentang prototipe Keamanan *Face Recognition Berbasis Principal Component Analisis* (PCA) dengan menggunakan metode *Fisherface* menghasilkan akurasi sebesar 85%, tetapi memiliki kelemahan untuk pengenalan wajah yang tidak dikenal sebesar 70% [2].

Dalam penelitian ini dipilih metode *eigenface* untuk metode pengenalan karena memiliki tingkat kesalahan lebih rendah dibandingkan dengan metode *fisherfish*. Kedua penelitian diatas dianggap masih memiliki kewanaman yang kurang karena tingkat keakurasian yang tergolong sedang dan tidak terdapat penambahan sistem keamanan. Penambahan keamanan dengan sebuah sistem yang dapat memberikan notifikasi langsung kepada pemilik ketika ada orang yang ingin membuka brankas dapat memberikan pengamanan ekstra. Dengan sistem yang seperti ini akan sangat mudah untuk mencegah terjadinya pencurian dan dapat memudahkan pemilik brankas untuk mengidentifikasi pelaku apabila telah terjadi pencurian. Selain itu pemilik dapat juga mengontrol langsung brankas dengan *handphone* untuk membuka ataupun menutup brankas melalui pesan telegram tentu dapat mempermudah pemilik untuk mengontrol brankas yang dimilikinya. Diharapkan dengan adanya prototipe ini nantinya dapat dikembangkan menjadi alat yang lebih baik dan dapat digunakan oleh masyarakat umum pada masa yang akan datang

METODE PENELITIAN

Metode penelitian penelitian ini menggunakan eksperimental. Dalam penelitian ini penulis melakukan percobaan secara langsung dalam pembuatan. Alat dan pengujian input, proses serta output, sehingga pengoperasian alat dapat dilakukan secara normal. Penelitian ini dibuat dalam enam tahapan yaitu dimulai dengan studi literatur, rancangan bangun alat, membuat skema alat, membuat algoritma *eigenface*, pengujian alat, hasil dan laporan, alur kerja penelitian dapat dilihat pada gambar 1. Alat dan bahan yang digunakan terdiri dari dua jenis, yaitu *hardware* dan *software*. Untuk alat dan bahan berupa *hardware* meliputi raspberry pi 3, kamera USB, *solenoid door lock*, modul *relay*, miniatur brankas, *buzzer*, dan laptop. Sedangkan *software* yang digunakan meliputi OS *raspberry jessie*, Python 3.7 (*IDLE*), *Library Opencv python v.4.5.1.48*, *Library dlib v19.21.1*, dan *library telebot v0.0.4*.

Gambar 1 Alur Penelitian dan Skematik



HASIL DAN PEMBAHASAN

Pengujian akurasi pencocokan wajah dilakukan untuk mengetahui akurasi sistem dalam mencocokkan wajah. Pengujian dilakukan dua tahapan, yaitu tahap pertama menguji citra sample yang sesuai dengan *database*, tahap kedua menguji citra sample yang tidak sesuai dengan *database*. Pengujian ini dilakukan secara real time menggunakan Raspberry Pi 3. Citra yang tersimpan pada *database* berupa data 2 orang dengan masing-masing 5 pose yang berbeda dengan intensitas cahaya yang sama. Perbedaan pose pada *database* terdiri dari posisi yang berbeda, yaitu menghadap depan, kiri 45°, kiri 90°, kanan 45° dan kanan 90°. Deteksi posisi wajah menggunakan *library dlib* dengan perintah untuk mendapatkan *crop* posisi wajah dan dijadikan sebagai sampel wajah. Sampel wajah selanjutnya diubah dalam warna grayscale untuk mengatasi efek *iluminasi*. Efek *iluminasi* merupakan efek yang disebabkan oleh sistem pencahayaan [10]. Dengan mengubah foto menjadi warna *grayscale* dapat meningkatkan keakuratan deteksi wajah [11]. Berikut sampel gambar yang digunakan untuk *database* wajah yang digunakan.

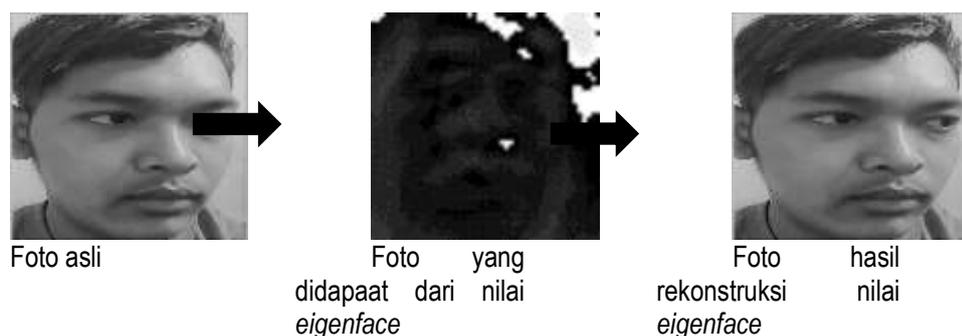
Gambar 2. Sampel wajah untuk *database* yang diubah menjadi *grayscale*

Setelah *database* didapatkan tahapan selanjutnya dalam pengenalan wajah ialah melatih sistem untuk mengenali wajah yang didaftarkan. Tahapan dalam pemrosesan pengenalan wajah ialah:

1. Foto diubah dalam ukuran yang sama yaitu 200 x 200 pixel
2. Foto diubah menjadi matrik sesuai dengan yang telah ditetapkan (dalam hal ini foto dirubah menjadi ukuran matrik 50x50)
3. Foto dikenali dari nilai *eigenface* yang didapatkan, selanjutnya disimpan dalam database.
4. Rekonstruksi foto dari nilai *eigenface* yang didapatkan.

Berikut proses yang terjadi dari foto yang diproses untuk menjadi database.

Gambar 5. Proses rekonstruksi wajah untuk database



Berdasarkan 10 kali percobaan didapatkan rata-rata waktu yang diperlukan untuk mengolah *database* adalah 0,623 detik. Tahapan selanjutnya setelah *database* diolah ialah proses pengenalan wajah melalui *webcam*. *Webcam* akan dibuat *stand-by* saat program dijalankan. Ketika sistem telah siap *webcam* akan mencari wajah dengan menggunakan *library dlib*, saat wajah telah ditemukan proses selanjutnya ialah mengambil gambar wajah dari *webcam* lalu diproses untuk dicari nilai *eigenface* nya dan dicocokkan dengan nama-nama yang telah terdaftar dalam *database*[12]. Berikut hasil percobaan pengenalan wajah yang telah dilakukan dengan pengujian menggunakan subjek sesuai dengan database yang terdaftar:

Tabel 1. Pengujian pengenalan wajah dengan metode *eigenface*

D	n ke-	Percobaa	Keterangan	Citra sebagai dikenali	Hasil pengujian
	1		Tampak depan	ID 1	Sesuai
	2		Tampak kiri 45°	ID 1	Sesuai
	3		Tampak kiri 90°	ID 1	Sesuai
	4	45°	Tampak kanan	ID 1	Sesuai
	5	90°	Tampak kanan	ID 1	Sesuai
	1		Tampak depan	ID 2	Sesuai
	2		Tampak kiri 45°	Tidak dikenal	Tidak sesuai
	3		Tampak kiri 90°	ID 2	Sesuai
	4	45°	Tampak kanan	ID 2	Sesuai
	5	90°	Tampak kanan	ID 2	Sesuai
	1		Tampak depan	Tidak dikenal	Sesuai
	2		Tampak kiri 45°	Tidak dikenal	Sesuai
	3		Tampak kiri 90°	Tidak dikenal	Sesuai
	4	45°	Tampak kanan	Tidak dikenal	Sesuai
	5		Tampak kanan	Tidak dikenal	Sesuai

		90°		
	1	Tampak depan	Tidak dikenal	Sesuai
	2	Tampak kiri 45°	Tidak dikenal	Sesuai
	3	Tampak kiri 90°	Tidak dikenal	Sesuai
	4	Tampak kanan 45°	Tidak dikenal	Sesuai
	5	Tampak kanan 90°	Tidak dikenal	Sesuai

Keakuratan sistem pengenalan wajah dapat dihitung dengan menggunakan rumus di sebagai berikut [13].

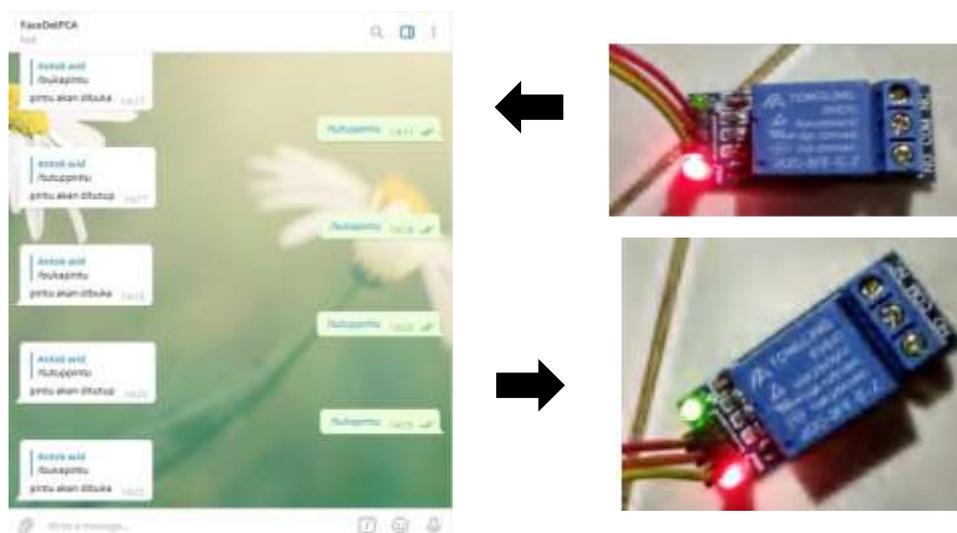
$$Keakuratan = \left(\frac{\text{jumlah data benar}}{\text{jumlah seluruh data}} \right) \times 100\%$$

Berdasarkan rumus diatas maka dapat dihitung keakuratan sistem pengenalan wajah berbasis PCA dengan metode *eigenface* adalah sebagai berikut:

$$Keakuratan = \left(\frac{19}{20} \right) \times 100\%$$

$$Keakuratan = 95\%$$

Dari hasil pengujian yang telah dilakukan didapatkan keakuratan sistem sebesar 95% dari hasil 20 total percobaan. Kesalahan dalam pengenalan wajah disebabkan karena sistem ini menggunakan pencocokan wajah dengan sampel *database* sesuai dengan nilai kesalahan terkecil, sehingga ketika foto yang didapatkan hampir mirip maka wajah tersebut dapat dikenali sebagai sampel dari *database*. Selain itu posisi kamera dengan wajah juga mempengaruhi keakuratan dalam pengenalan wajah, tingkat kecerahan foto juga ikut andil dalam menentukan hasil yang didapatkan. Selain itu resolusi citra sample yang didapat *random* artinya setiap terdeteksi wajah maka akan langsung tersimpan tanpa ada pengaturan resolusi citra yang tetap[14].



Gambar 6 . Proses pengujian relay via telegram

Berdasarkan hasil pengujian, diketahui bahwa *delay* pengendalian *relay* melalui perintah yang dikirimkan dari Telegram memiliki rata-rata *delay* waktu sebesar 1,30 detik. Dengan waktu *delay* tercepat adalah 0,84 detik dan waktu *delay* terlama adalah 1,3 detik. *Delay* ini terjadi akibat adanya pengaruh dari kecepatan internet. Selanjutnya dilakukan pengujian secara keseluruhan, pengujian secara keseluruhan bertujuan untuk mengetahui ketepatan pencocokan wajah dan *delay* waktu sistem sampai dengan pengendalian relay. Pengujian dilakukan sebanyak 10 kali oleh subjek yang terdaftar pada *database*. Pengambilan data dilakukan secara *realtime* melalui webcam dengan deteksi pertama serta dilakukan pengulangan mulai sistem. Pengurangan nilai kecocokan dilakukan agar meningkatkan keakuratan sistem. Untuk menghitung waktu proses keseluruhan digunakan

stopwatch dengan mencatat waktu awal program dijalankan sampai terkendalinya relay. Berikut ini adalah tabel pengujian sistem kerja alat secara keseluruhan:

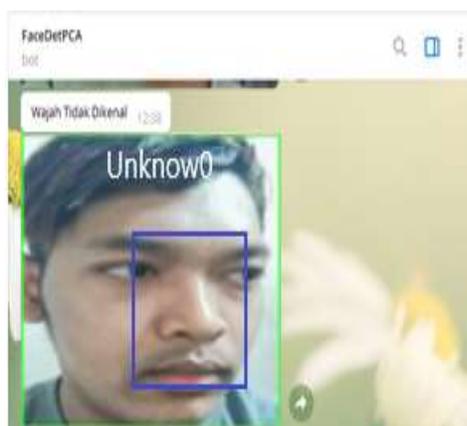
Tabel 2 . Hasil pengujian alat secara keseluruhan

o	Sample	Citra dikenali	Berhasil	Relay	Waktu respon (detik)
	ID 1	Citra ID 1	Ya	bah Beru	14,01
		Citra ID 1	Ya	bah Beru	14,70
		Citra ID 1	Ya	bah Beru	13,91
		Citra ID 1	Ya	bah Beru	14,31
		Citra ID 1	Ya	bah Beru	14,56
	ID 2	Citra ID 2	Ya	bah Beru	13,87
		Citra ID 2	Ya	bah Beru	13,97
		Citra ID 2	Ya	bah Beru	14,06
		Citra ID 2	Ya	bah Beru	14,12
0		Citra ID 2	Ya	bah Beru	14,21
	Rata-rata				14,17

Berdasarkan 10 kali percobaan citra wajah dengan subjek terdaftar mendapatkan keakuratan 100%. Hal ini dapat dilihat bahwa tidak terdapat kesalahan dalam pencocokan wajah dari citra subjek yang telah terdaftar. Waktu rata-rata yang diperlukan untuk mengenali wajah sampai dengan perubahan pada relay adalah 14,17 detik. Lama waktu pemrosesan wajah tergantung pada jumlah *database* dan ukuran dari file yang diproses pada *database*. Jumlah sampel yang tidak terlalu banyak juga dapat meningkatkan keakuratan dari hasil pencocokan wajah dengan citra yang tersimpan pada *database*. Selain itu banyaknya *library* yang harus diimpor untuk menjalankan *script* juga mempengaruhi lama waktu pemrosesan wajah, karena memerlukan waktu *booting* aplikasi yang lebih lama[15].

Pengujian *delay* pengiriman data melalui aplikasi *telegram* dilakukan pada citra yang tidak terdaftar pada *database*. Pengujian ini bertujuan untuk mengetahui *delay* waktu pengiriman foto dan pemberitahuan dari aplikasi ke telegram. Foto yang dikirim merupakan citra wajah tidak terdaftar yang mencoba untuk membuka brankas, berikut tampilan *notifikasi* pada aplikasi *telegram*.

Gambar 7 Citra dan teks pada telegram



Sama dengan pengujian secara keseluruhan, pengambilan data pengujian delay pengiriman data ke telegram secara *real time* melalui WebCam dengan deteksi pertama serta dilakukan pengulangan mulai sistem. Untuk menghitung waktu proses pengiriman digunakan stopwatch dari awal program dijalankan sampai citra dan teks terkirim ke Telegram. Berikut hasil pengujian *delay* pengiriman data citra dan teks ke aplikasi telegram.

Tabel 3
Hasil pengujian delay pengiriman data ke Telegram

I ke-	Sampe	Status data	Keterangan	Delay waktu pengiriman (detik)
1		Terkirim	Berhasil	15,60
2		Terkirim	Berhasil	14,41
3		Terkirim	Berhasil	16,07
4		Terkirim	Berhasil	15,42
5		Terkirim	Berhasil	14,21
6		Terkirim	Berhasil	13,20
7		Terkirim	Berhasil	13,45
8		Terkirim	Berhasil	14,21
9		Terkirim	Berhasil	15,43
10		Terkirim	Berhasil	15,02
	Rata-rata			14,70

Berdasarkan 10 kali percobaan, semua data dapat terkirim dengan baik ke Telegram. Waktu pengiriman bervariasi dari 13,20 detik sampai dengan 16,07 detik dengan rata-rata waktu pengiriman 14,70 detik. Banyaknya *library* yang harus diimport pada sistem menjadi faktor utama dari lamanya waktu *booting system* dan aplikasi dari awal dinyalakan. Selain itu aplikasi juga memerlukan waktu untuk memproses database untuk dapat mengenali wajah yang akan diuji. Koneksi internet dan besarnya data yang dikirim juga menjadi faktor penting dalam menentukan waktu *delay* pengiriman data ke telegram.

KESIMPULAN

Dengan menggunakan algoritma PCA dengan perhitungan *eigenface* akurasi pencocokan citra wajah yang terdaftar sebesar 95% dari total 20 kali percobaan, dimana 10 kali percobaan dengan menggunakan wajah yang terdaftar dan 10 kali percobaan dengan menggunakan wajah yang tidak terdaftar dalam database. Pengendalian *relay* menggunakan telegram memiliki waktu *delay* rata-rata 1,11 detik. Hal ini menunjukkan bahwa pengendalian kunci brankas dengan menggunakan telegram merupakan salah satu sistem dengan waktu delay yang rendah, dan ini sangat efektif. Kinerja alat secara keseluruhan memerlukan waktu sekitar 14,17 detik untuk dapat mengenali wajah dari awal *booting* aplikasi, sedangkan *delay* waktu pengiriman data citra wajah yang tidak cocok ke telegram memerlukan waktu sekitar 14,70 detik. Lama pengenalan wajah ini disebabkan karena

waktu *booting* aplikasi yang cukup lama pada awal dinyalakan dikarenakan *import library* pada sistem, akan tetapi ketika memasuki waktu *stand-by* waktu yang diperlukan untuk mengenali wajah relatif lebih singkat.

LITERATUR

- Mulyadi, Andi Hary, Lapodje T., Armin L. 2012. "Pengenalan Citra Wajah Menggunakan Metode Analisis Komponen Utama dan Jarak Euclidean". Makasar: Universitas Hassanudin
- Kurniawan, Rudi dan A. Zulus, 2019. "Smart Home Security menggunakan Face Recognition dengan Metode Eigenface Berbasis Raspberry Pi" Lubuklinggau: Jurnal Sustainable.
- Septian, Kevin Dwi, Ismail S.J.I., Anang S. 2019. "Prototipe sistem keamanan Face Recognition Berbasis Principal Component Analisis (PCA)". E-proceeding of Applied Science: vol.5, No.2, ISSN: 2442-5826
- Turk, M. & Pentland, A. 1991. "Eigenfaces for Recognition". Journal of Cognitive Neuroscience. Vol 3, No. 1. 71-86.
- Suprianto, Dodit, Rini N.H., Purnomo B.S. 2013. "Sistem Pengenalan Wajah Secara Realtime dengan Adaboost, Eigenface PCA & MySQL. Jurnal EECCIS Vol.7 No.2.
- Gan, J.-y., Zhou, D.-p. & Li, C.-z., 2005. AAA Method For Improved PCA in Face Recognition. International Journal of Information Technology, 11(11), pp. 79- 85.