



Hak cipta dan penggunaan kembali:

Lisensi ini mengizinkan setiap orang untuk menggubah, memperbaiki, dan membuat ciptaan turunan bukan untuk kepentingan komersial, selama anda mencantumkan nama penulis dan melisensikan ciptaan turunan dengan syarat yang serupa dengan ciptaan asli.

Copyright and reuse:

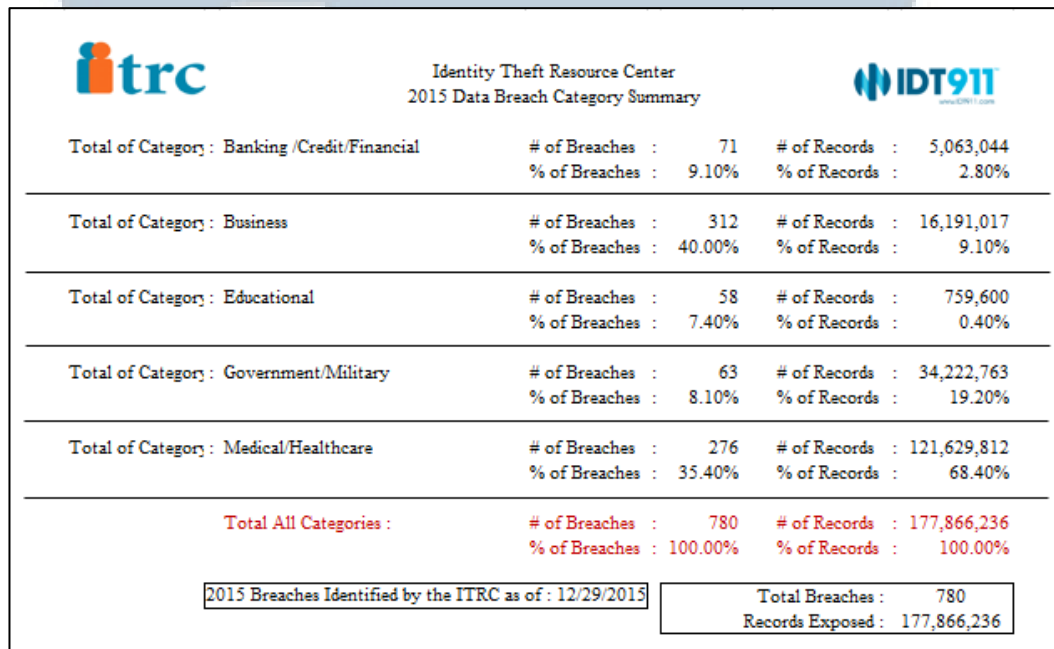
This license lets you remix, tweak, and build upon work non-commercially, as long as you credit the origin creator and license it on your new creations under the identical terms.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan pada sebuah sistem atau aplikasi masih terbilang rendah, didukung dengan adanya statistik yang dikeluarkan oleh *Identity Theft Resource Center* (ITRC) pada tanggal 29 Desember 2015 pada Gambar 1.1. Pada gambar tersebut terdapat 780 sistem yang berhasil dibobol dan terdapat 177,866,236 data yang berhasil diakses.



The image shows a table titled 'Identity Theft Resource Center 2015 Data Breach Category Summary'. It lists various categories of data breaches, including Banking/Credit/Financial, Business, Educational, Government/Military, and Medical/Healthcare. For each category, it provides the number of breaches, the percentage of breaches, the number of records exposed, and the percentage of records. A total row at the bottom shows 780 breaches and 177,866,236 records exposed. A box at the bottom right states 'Total Breaches: 780' and 'Records Exposed: 177,866,236'. A box at the bottom left states '2015 Breaches Identified by the ITRC as of: 12/29/2015'.

Category	# of Breaches	% of Breaches	# of Records	% of Records
Total of Category : Banking /Credit/Financial	71	9.10%	5,063,044	2.80%
Total of Category : Business	312	40.00%	16,191,017	9.10%
Total of Category : Educational	58	7.40%	759,600	0.40%
Total of Category : Government/Military	63	8.10%	34,222,763	19.20%
Total of Category : Medical/Healthcare	276	35.40%	121,629,812	68.40%
Total All Categories :	780	100.00%	177,866,236	100.00%

2015 Breaches Identified by the ITRC as of: 12/29/2015

Total Breaches : 780
Records Exposed : 177,866,236

Gambar 1.1 Statistik Identity Theft Resource Center (ITRC, 2015:4)

Hal tersebut dikarenakan kurangnya kualitas *authentication* yang dimiliki oleh sistem tersebut. *Authentication* memiliki 3 (tiga) tipe yaitu *something you know*, *something you have*, *something you are* (Liu & Silverman, 2001:27). *Something you know* merupakan sesuatu yang diketahui oleh pengguna seperti *password* atau *Personal Information Number* (PIN). *Something you have*

merupakan sesuatu yang dimiliki oleh pengguna seperti passport, Kartu Tanda Penduduk (KTP) dan kartu Anjungan Tunai Mandiri (ATM). *Something you are* menggunakan keunikan dari pengguna dan biasa dikenal dengan *biometry security*.

Biometric berasal dari Bahasa Yunani yang terdiri dari 2 (dua) kata “*bio*” yang berarti kehidupan dan “*metric*” yang berarti mengukur. *Biometric* merupakan pengenalan pola dengan menggunakan fisik ataupun perilaku dari pengguna dan bertujuan untuk mengidentifikasi identitas dari pengguna (Jain, 2000:92). *Face Recognition* merupakan salah satu cara dari pengenalan pola pada *biometric* dengan menggunakan fisik dari pengguna. *Face recognition* mulai mendapatkan perhatian yang signifikan dikarenakan 2 (dua) alasan yaitu berkembangnya aplikasi komersial dan ketersediaan teknologi yang layak setelah penelitian yang dilakukan selama 30 tahun (Zhao, 2003:400).

Face recognition terdapat 2 jenis pendekatan yaitu *2D face recognition* dan *3D face recognition*. *2D face recognition* (berbasis citra atau gambar) mudah dipengaruhi oleh keadaan lingkungan, orientasi wajah, ekspresi wajah, dan dandanan. Oleh karena itu, penggunaan data 3D akan sangat membantu untuk dapat mengatasi masalah *intrinsic* yang dimiliki oleh pendekatan 2D (Bronstein A. & Bronstein M., 2003:62). Maka dari itu penelitian ini membahas tentang pemodelan objek tiga dimensi pada sistem keamanan dengan mengimplementasikan algoritma *Direct Linear Transformation* (DLT). DLT merupakan merupakan algoritma yang dapat menentukan koordinat 3D dari sebuah titik yang didapatkan dari beberapa citra 2D. Menurut Phillippe Pourcelot dalam jurnal yang berjudul “A Method to synchronise cameras using the direct linear transformation technique” mengatakan bahwa DLT biasa digunakan pada analisis kinematika dari pergerakan manusia

serta hewan dikarenakan memiliki hasil keakuratan yang tinggi pada penentuan koordinat 3D serta memiliki fleksibilitas yang besar dalam pengaturan kamera (2000:1751).

1.2 Rumusan Masalah

Berdasarkan latar belakang permasalahan di atas, maka rumusan masalah pada penelitian ini adalah bagaimana mengimplementasikan algoritma *Direct Linear Transformation* untuk pemodelan wajah tiga dimensi dalam *authentication*?

1.3 Batasan Masalah

Batasan masalah pada penelitian ini adalah menggunakan *library* EmguCV pada proses kalibrasi kamera, *library* FaceLuxand SDK pada proses *face detection*, dan *library* Neural Network pada proses *face recognition*.

1.4 Tujuan Penelitian

Berdasarkan latar belakang permasalahan di atas, maka tujuan dari penelitian ini adalah mengimplementasikan algoritma *Direct Linear Transform* untuk pemodelan wajah tiga dimensi dalam *authentication*.

1.5 Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini adalah membantu masyarakat untuk meningkatkan keamanan pada suatu sistem atau aplikasi.

1.6 Sistematika Penulisan

Penelitian ditulis dengan sistematika penulisan sebagai berikut.

1. BAB I Pendahuluan

Pendahuluan berisikan latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan pada penelitian.

2. BAB II Landasan Teori

Berisikan landasan dari teori-teori yang digunakan pada penelitian antara lain adalah kalibrasi kamera, *face detection*, *Direct Linear Transformation (DLT)*, *face recognition*, *False Acceptance Rate (FAR)*, dan *False Rejection Rate (FRR)*.

3. BAB III Metodologi dan Perancangan Sistem

Berisikan metode penelitian yang digunakan yaitu studi literatur, analisis sistem, perancangan sistem, pemrograman sistem, dan pengujian.

4. BAB IV Implementasi dan Uji Coba

Berisikan hasil uji coba yang dilakukan pada algoritma dan aplikasi yang telah dirancang dan diprogram.

5. BAB V Simpulan dan Saran

Simpulan dari hasil penelitian yang telah dirancang, diprogram dan diuji coba akan ditulis serta memberikan saran yang ditujukan pada penelitian selanjutnya.

