Teknologi Biometrik:

Impementasi pada Bidang Medis Menggunakan Matlabs

UU No 28 tahun 2014 tentang Hak Cipta

Fungsi dan sifat hak cipta Pasal 4

Hak Cipta sebagaimana dimaksud dalam Pasal 3 huruf a merupakan hak eksklusif yang terdiri atas hak moral dan hak ekonomi.

Pembatasan Pelindungan Pasal 26

Ketentuan sebagaimana dimaksud dalam Pasal 23, Pasal 24, dan Pasal 25 tidak berlaku terhadap:

i. penggunaan kutipan singkat ciptaan dan/atau produk hak terkait untuk pelaporan peristiwa aktual yang ditujukan hanya untuk keperluan penyediaan informasi aktual;
ii. penggandaan ciptaan dan/atau produk hak terkait hanya untuk kepentingan penelitian ilmu pengetahuan;
iii. penggandaan ciptaan dan/atau produk hak terkait hanya untuk keperluan pengajaran, kecuali pertunjukan dan fonogram yang telah dilakukan pengumuman sebagai bahan ajar; dan
iv. penggunaan untuk kepentingan pendidikan dan pengembangan ilmu pengetahuan yang memungkinkan suatu ciptaan dan/atau produk hak terkait dapat digunakan tanpa izin pelaku pertunjukan, produser fonogram, atau lembaga penyiaran.

Sanksi Pelanggaran Pasal 113

1. Setiap orang yang dengan tanpa hak melakukan pelanggaran hak ekonomi sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf i untuk penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 1 (satu) tahun dan/atau pidana denda paling banyak Rp100.000.000 (seratus juta rupiah).
2. Setiap orang yang dengan tanpa hak dan/atau tanpa izin pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf c, huruf d, huruf f, dan/atau huruf h untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 3 (tiga) tahun dan/atau pidana denda paling banyak Rp500.000.000,00 (lima ratus juta rupiah).

Implementasi pada Bidang Medis Menggunakan Matlabs

Dr. Ir. Sumijan, M.Sc.
Pradani Ayu Widya Purnama, S.Kom., M.Kom.
Syafri Arlis, S.Kom., M.Kom.

PT Insan Cendekia
Mandiri Group

Teknologi Biometrik:
Implementasi pada Bidang Medis Menggunakan Matlabs

Dr. Ir. Sumijan, M.Sc.
Pradani Ayu Widya Purnama, S.Kom., M.Kom.
Syafri Arlis, S.Kom., M.Kom.

Editor :
Siti Jamalul Insani dan Yahya Alhidayah

Desainer:
Mifta Ardila

Sumber :
www.insancendekiamandiri.co.id

Penata Letak:
Siti Jamalul Insani

Proofreader :
Tim ICM

Ukuran :
xiv, 202 hlm., Uk: 14,8x21 cm

ISBN :
978-623-348-496-1

Cetakan Pertama :
Desember 2021

Hak Cipta 2021, pada
Dr. Ir. Sumijan, M.Sc.
Pradani Ayu Widya Purnama, S.Kom., M.Kom.
Syafri Arlis, S.Kom., M.Kom.

Isi di luar tanggung jawab penerbitan dan percetakan

Hak cipta dilindungi undang-undang
Dilarang keras menerjemahkan, memfotokopi, atau
memperbanyak sebagian atau seluruh isi buku ini
tanpa izin tertulis dari Penerbit.

Anggota IKAPI : 020/SBA/20

PENERBIT INSAN CENDEKIA MANDIRI
(Grup Penerbitan PT INSAN CENDEKIA MANDIRI)

Perumahan Gardena Maisa 2, Blok F03, Nagari Koto Baru, Kecamatan Kubung,
Kabupaten Solok, Provinsi Sumatra Barat – Indonesia 27361
HP/WA: 0813-7272-5118
Website: www.insancendekiamandiri.co.id
www.insancendekiamandiri.com
E-mail: penerbitbic@gmail.com

Daftar Isi

Daftar Gambar

Daftar Tabel

Prakata

Teknologi biometrik adalah sebuah metode komputerisasi yang menggunakan aspek-aspek biologi terutama karakte-ristik yang unik dan spesifik yang dimiliki oleh manusia. Karakterisitik fisiologi unik yang dapat digunakan sidik jari, wajah, tangan, iris, retina, suara, tanda tangan, cara penge-tikan. Perangkat presensi dapat mengenali sidik jari para mahasiswa yang akan mengikuti kuliah. Pintu pun terbuka setelah retina mata si pegawai dipindai oleh pembaca retina mata. Hal-hal tersebut menunjukkan beberapa contoh yang melibatkan pengolahan citra.

Saat ini telah banyak berkembang peralatan teknologi akuisisi citra medis, salah satu di antaranya adalah teknologi yang lazim disebut CT-scan. CT-Scan (*Computed Tomography Scan*) adalah suatu prosedur yang digunakan untuk mendapatkan gambaran dari berbagai area kecil dari tulang termasuk tengkorak kepala dan otak. Citra hasil akuisisi atau rekaman CT-Scan dapat mebantu memperjelas adanya dugaan yang kuat tentang kelainan yang terjadi pada otak, misalnya: gambaran lesi dari tumor, hematoma dan abses, pendarahan pada otak serta perubahan vaskuler berupa malformasi, naik turunnya vaskularisasi dan infark.

Peralatan sistem CT-Scan terdiri atas tiga bagian, yaitu Sistem Akuisisi Citra, Sistem Komputer dan Kendali, Stasiun Operasi dan Stasiun Pengamat. CT-Scan bekerja dalam sistem akuisisi citra terdapat dalam *frame* pipa dari mesin dan merupakan bagian sistem yang langsung berhadapan dengan pasien. Scanner terdiri atas sumber sinar-x, collimator, detektor, dan bagian akuisisi data.

Magnetic resonance imaging (MRI) adalah pemeriksaan bersifat diagnostik yang paling umum digunakan untuk mende-

teksi adanya tumor otak dan mendiagnosa kanker otak. Pemeriksaan ini bekerja dengan menempatkan pasien pada medan magnet dan menggunakan energi gelombang radio untuk mengambil gambar dari otak di dalam kepala. MRI merupakan pemeriksaan bersifat diagnostik yang lebih canggih daripada pemeriksaan normal sinar-X, USG, atau CT (tomografi komputer) karena dapat memberikan informasi luas yang tidak dapat diberikan pemeriksaan pencitraan lainnya.

Para penulis buku ini adalah lulusan Program Pacasarjana yang mendalami kajian Teknologi Informasi dan Komunikasi (dari aspek perilaku pengguna sistem dan pengelola sistem), dan saat ini menjadi dosen tetap di Fakultas Ilmu Komputer, Univeristas Putra Indonesia "YPTK" Padang. Latar belakang salah satu penulis bergelar Doktor Teknologi Informasi *(DTI)* menjadi salah satu elemen yang memperkaya kajian dan paparan dalam buku ini.

Akhirnya kami ucapkan selamat kepada para penulis atas terbitnya buku ini dan semoga buku ini bermanfaat bagi pembaca yang ingin belajar pengolahan citra digital dan penerapannya di bidang citra medis. Mudah-mudahan para penulis terus berkiprah dalam penulisan buku dan buku-buku yang lainnya serta pengembangan ilmu khususnya bidang Teknologi Informasi dan Komunikasi sesuai dengan perkembangan ilmu dan teknologi informasi saat ini berkembang pesat, akhirnya penulis memohon kepada pembaca buku ini jika ada masukan saran dan kritikan dalam buku ini silahkan di email: soe@upiyptk.org/sumijan@upiyptk.ac.id.

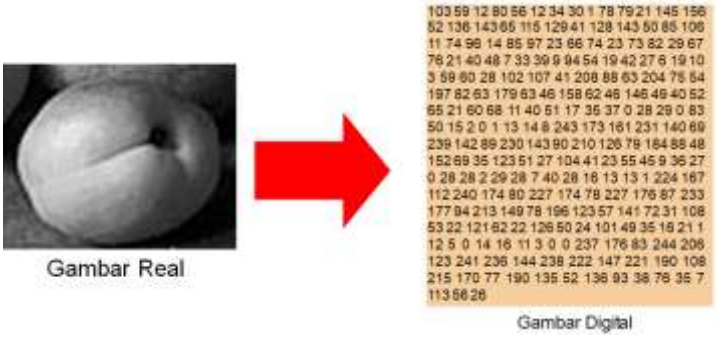
Padang, Desember 2021

Penulis

01 Teknologi Citra Digital

A. Dasar Citra Digital

Citra diartikan sebagai suatu fungsi intensitas cahaya, Dua dimensi, yang dinyatakan oleh f(x,y), di mana nilai atau amplitude dari f pada koordinat spasial (x,y) menyatakan intensitas (kecerahan) citra pada titik tersebut (Gonzalez dan Woods, 2008), Citra digital merupakan fungsi intensitas cahaya f(x,y), dimana harga x dan y merupakan koordinat spasial dan harga fungsi tersebut pada setiap titik (x,y) merupakan tingkat kecemerlangan citra pada titik tersebut; Citra digital merupakan suatu matriks dimana indeks baris dan kolomnya menyatakan letak suatu titik pada citra tersebut dan tingkat keabuan.



Gambar 1.1. Visualisasi Citra Digital dari Data Citra Real

Citra atau Image merupakan istilah lain dari gambar, yang merupakan informasi berbentuk visual. Citra ada dua (2) macam:

a) Citra Kontinu: dihasilkan dari sistem optik yang menerima sinyal analog : Contoh : Mata manusia, kamera analog.
b) Citra Diskrit: dihasilkan melalui proses digitalisasi terhadap citra continue Contoh : Kamera digital, scanner.

1. Representasi Citra Digital

a. Bitmap

1) Dipresentasikan dalam bentuk matrik, atau dipetakan dengan menggunakan bilangan biner.
2) Gambar Bitmap dipresentasikan dalam bentuk matrik, atau dipetakan dengan menggunakan bilangan binner atau sistem bilangan lain, memiliki kelebihan untuk memanipulasi warna namun untuk merubah objek lebih sulit.

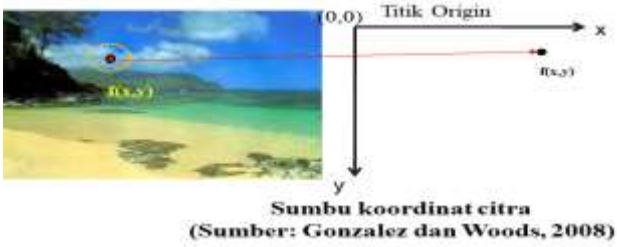
b. Grafik

1) Gambar grafik data tersimpan dalam bentuk vektor posisi.
2) Gambar grafik data tersimpan dalam bentuk vektor posisi, di mana yang tersimpan hanya informasi vektor posisinya dengan bentuk sebuah fungsi, lebih sulit dalam merubah warna tapi lebih mudah membentuk objek.

a. Penampilan citra secara visual nilai data digital yang disimpan oleh komputer, merepresentasikan warna dari citra yang diolah.
b. Citra biner (monokrom): setiap titik bernilai 0 untuk warna hitam atau 1 untuk warna putih. Satu titik pada

citra hanya membutuhkan satu bit. Citra skala keabuan (*gray scale*): peluang warna lebih banyak dibanding citra biner. Contoh: u/ skala keabuan 4 bit, maka jumlah kemungkinan nilainya adalah 2^4 = 16, dan nilai maksimumnya adalah 16-1.

c. Citra Warna (*true color*): pada citra warna, setiap titik mempunyai warna yang spesifik yang merupakan kombinasi dari 3 warna dasar RGB. Setiap warna dasar mempunyai intensitas dengan nilai maksimum 255 (8 bit). Contoh: kuninng merupakan kombinasi dari merah dan hijau sehingga nilai RGB nya adalah: 255 255 0.



Gambar 1.2. Pemetaan Visualisasi Citra Digital & Sumbu Koordinat

Gambar 1.3. Pemetaan Visualisasi Citra Digital RGB

2. Komponen Citra Digital

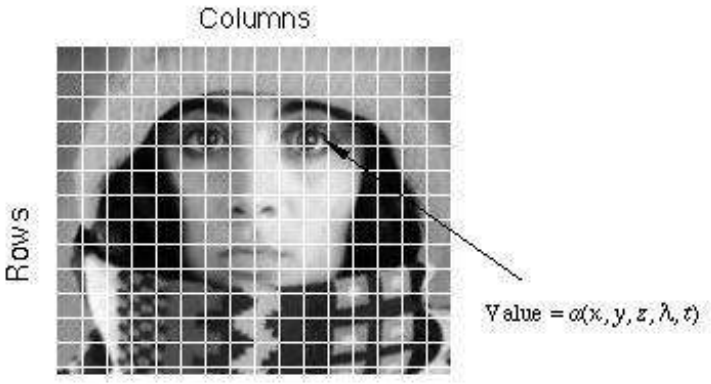
a. Piksel (titik)
b. Warna (instensitas)
c. Resolusi (kerapatan)
d. Brightness (cerah)
e. Contrast (terang)
f. Countour (perubahan instensitas)
g. Sharp (bentuk citra)
h. Texture (permukaan suatu citra)

a. *Pixel* dari citra yang dapat ditangkap oleh sistem penglihatan.
b. *Color,* warna sebagai persepsi yang ditangkap sistem visual terhadap panjang *brightness*, kecerahan atau intensitas cahaya yang dipancarkan
c. *Contrast,* kontras menyatakan sebaran terang *"lightness"* dan gelap *"darkness"* di dalam gambar.
d. *Contour*, kontur merupakan keadaan yang ditimbulkan oleh perubahan intensitas pada pixel yang bertetang-gaan.
e. Gelombang cahaya yang dipantulkan oleh objek.
f. *Sharp*, bentuk sebagai properti instristik dari objek 3 dimensi.
g. *Texture*, tekstur dicirikan sebagai distribusi spasial sari derajat keabuan di dalam sekumpulan pixel yang bertetanggaan.
h. *Resolusi :* resolusi mengacu pada jumlah piksel dalam gambar, resousi juga diidentifikasi oleh lebar dan tinggi gambar, serta jumlah piksel dalam gambar. Sebagai contoh: sebuah gambar memiliki 2048 piksel pada ukuran lebar dan 1536 piksel pada ukuran tinggi, atau

berisi 2.048x1.536 = 3.145.728 piksel (atau 3.1 megapixels).

3. Pengolahan Citra Digital

Pengolahan citra digital adalah kegiatan memperbaiki kualitas citra maupun memanipulasi citra agar mudah diinterpretasi oleh manusia/mesin (komputer).



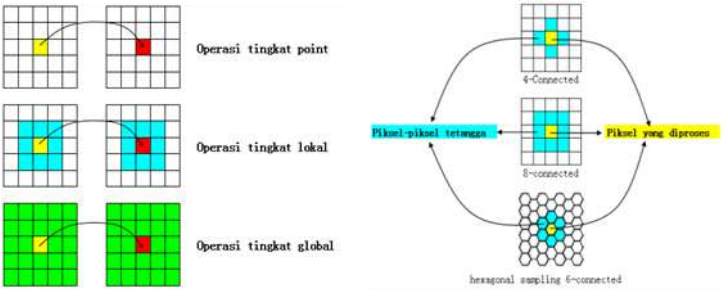
Gambar 1.4. Matrik Citra Digital X (Columns x Rows)

a. Operasi tingkat point
   1) Operasi pada suatu piksel pada suatu koordinat yang tidak tergantung pada piksel-piksel tetangganya.
   2) Nilai *output* hanya tergantung nilai-nilaiyang dimiliki piksel itu sendiri.

b. Operasi tingkat lokal
   1) Operasi pada suatu piksel pada suatu koordinat yang tergantung pada piksel- piksel tetangganya.

c. Operasi tingkat global
   1) Operasi pada suatu koordinat yang tergantung pada nilai-nilai piksel yang terkandung pada keseluruhan citra.

d. Operasi tingkat objek
   1) Operasi yang dilakukan pada piksel-piksel yang dikenali ataupun akan dikenali sebagai suatu objek.



Gambar 1.5. Jenis Operasi dalam citra digital

4. Operasi-operasi pada pengolahan citra

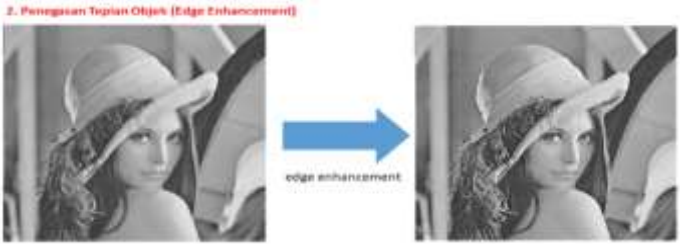
a. Perbaikan kualitas citra (*image enhancement*)

Tujuan perbaikan kualitas citra *(image enhancement)* adalah untuk menonjolkan suatu ciri tertentu dalam citra tersebut, ataupun untuk memperbaiki aspek tampilan. Operasi titik dalam *image enhancement* dilakukan dengan memodifikasi histogram citra masukan agar sesuai dengan karakteristik yang diharapkan. Perbaikan kualitas citra digital, meliputi :

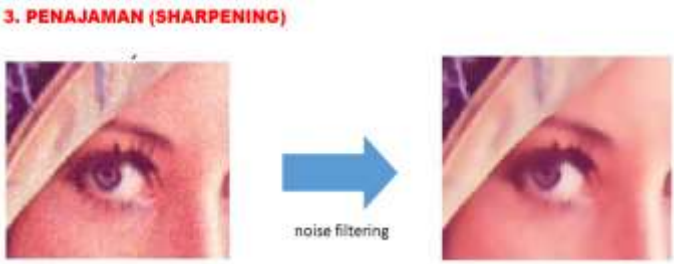
1) pengaturan kontras
2) penegasan tepian objek (edge enhancement)
3) penajaman (sharpening)

4) pemberian warna semu (pseudocoloring)
5) pemfilteran derau (noise filtering)

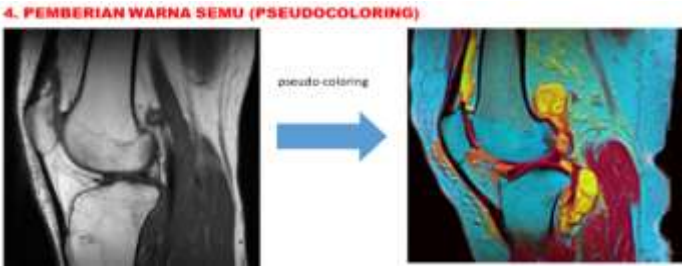
Gambar 1.6. Hasil operasi kontras pada citra digital



Gambar 1.7. Hasil operasi penegasan tepi pada citra digital



Gambar 1.8. Hasil operasi penajaman pada citra digital



Gambar 1.9. Hasil operasi pemberian warna semu pada citra digital

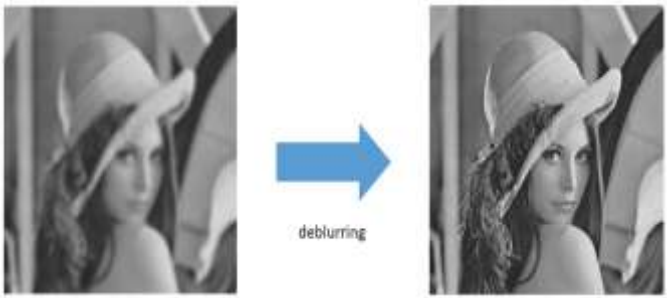
Gambar 1.10. Hasil Operasi Pemilteran Derau pada citra digital

b. Restorasi citra, meliputi :

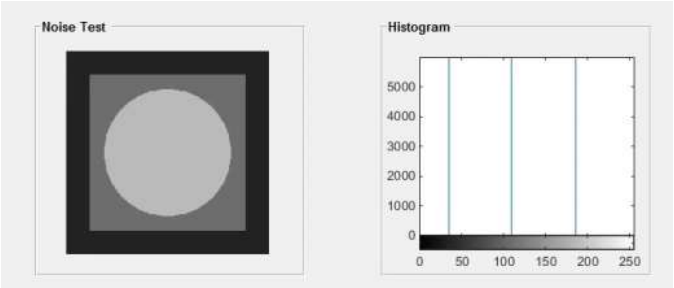
Dalam dunia nyata, suatu proses pencitraan hampir dapat dipastikan akan menghasilkan citra keluaran yang mengalami degradasi. Penyebab degradasi ini antara lain berupa sensor yang tidak fokus, pergerakan dari objek maupun sistem pencitraan, gangguan derau termal pada sensor dan perangkat elektronik sistem pencitraan, maupun sebab-sebab lainnya yang terkait dengan lingkungan pengambilan data seperti turbulensi atmosfir pada praktik *remote sensing* dan pengamatan astronomi. Untuk memperoleh citra yang lebih tepat, diperlukan adanya suatu proses restorasi citra.

Restorasi citra berkaitan dengan upaya memperoleh kembali suatu citra asal dari sebuah citra yang terdegradasi, dengan memanfaatkan suatu pengetahuan mengenai proses terjadinya degradasi tersebut. Restorasi citra (*image restoration*) dapat dibedakan dengan perbaikan citra (*image enhancement*), di mana proses yang dilakukan dalam perbaikan citra lebih bersifat heuristik dan lebih dititikberatkan pada upaya melakukan aksentuasi fitur dalam citra. Beberapa proses restorasi citra, di antaranya:

1) Penghilangan kesamaran *(deblurring)*
2) Penghilangan derau *(noise)*



Gambar 1.11. Hasil Operasi Kesamatan pada citra digital



Gambar 1.12. Hasil Operasi Penghilangan Derau pada citra digital

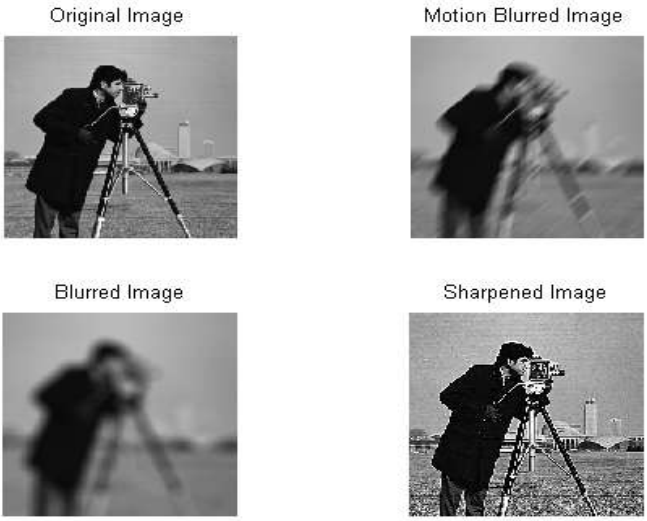
B. Pengolahan Citra Digital

Secara singkat pengolahan citra digital yaitu suatu kegiatan mengolah citra digital agar menjadi citra digital baru. Secara detail pengolahan citra digital yaitu suatu kegiatan mengolah atau mengubah citra digital agar menjadi citra digital baru supaya mudah untuk dianalisis, dilihat, dan dipahami sehingga kualitas citra menjadi lebih baik, dan lebih informatif. Berikut adalah beberapa operasi pengolahan citra digital:

1. Perbaikan kualitas citra *(image enhancement)*

Image enhancement bertujuan untuk memperbaiki kualitas citra dengan cara memanipulasi parameter-parameter citra. Dengan operasi ini, ciri-ciri khusus yg terdapat dalam citra lebih ditonjolkan. Contoh pengolahan citra dengan *image enhancement* adalah perbaikan kontras gelap/ terang, perbaikan tepian objek (*edge enhancement*), penajaman (*sharpening*), pemberian warna semu (*pseudocoloring*), penapisan derau (*noise filtering*).

Gambar 1.13. Contoh gambar yang telah dilakukan penajaman



Gambar 1.14. (a) Citra cameraman asli, (b) Citra cameraman kabur saat pengambilan gambar kamera bergoyang, (c) Citra cameraman kabur krn pengaturan lensa tdk fokus, (d) Citra cameraman setelah ditajamkan.

2. Pemugaran citra *(image restoration)*

Bertujuan menghilangkan/meminimumkan cacat pada citra. Tujuan hampir sama dengan operasi perbaikan citra, bedanya, pada pemugaran citra penyebab degradasi gambar diketahui. Contoh dari pemugaran citra adalah penghilangan kesamaran *(deblurring)* dan penghilangan derau.

Gambar 1.15. Citra cameramen yang kabur di olah menggunakan pengolahan deblurring menjadi citra yang tidak kabur.

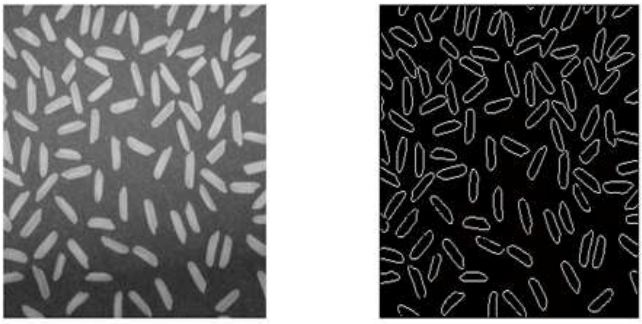
3. Pemampatan *image (image compression)*

Tujuan dari pemampatan *image* adalah agar citra dapat direpresentasikan lebih kompak shg memerlukan memori yg lebih sedikit, namun citra harus tetap mempunyai kualitas gambar yg bagus .

Gambar 1.16. citra cameraman.bmp (192 KB) sebelum dimampatkan,menjadi citra cameraman.jpg (11 KB) setelah dimampatkan

4. **Segmentasi citra *(image segmentation)***
   Untuk memecah suatu citra ke dalam beberapa segmen dengan suatu kriteria tertentu. Jenis operasi ini berkaitan erat dengan pengenalan pola.

5. **Pengorakan citra *(image analysis)***
   Bertujuan menghitung besaran kuantitatif dari citra untuk menghasilkan deskripsinya. Mengekstraksi ciri-ciri tertentu yang membantu dalam identifikasi objek. Proses segmentasi kadang diperlukan untuk melokalisasi objek yg diinginkan dari sekelilingnya. Contoh dari pengolahan *image analysis* adalah deteksi tepi, ekstrasi batas, dan ekstrasi daerah.



Gambar 1.17. Citra *rice* yang kemudian dilakukan pengolahan citra deteksi tepi

6. **Rekonstruksi citra *(image reconstruction)***
   Image reconstruction bertujuan membentuk ulang objek dari beberapa citra hasil proyeksi. Banyak digunakan dalam bidang medis. Misal beberapa foto *rontgen* dgn sinar X digunakan utk membentuk ulang gambar organ tubuh.

C. Dasar *Noise* dan *Filtering*

Noise memiliki pengertian yang banyak (tidak ada hanya dalam pencitraan). Dalam pencitraan noise berarti variasi kecerahan atau informasi warna pada gambar. noise bisa diproduksi oleh sensor dan sirkuit pemindai atau kamera digital. Noise juga bisa berasal dari butiran fosfor film dan penyebab noise yang demikian tidak dapat dihindari . image noise adalah Produk sampingan yang tidak diinginkan dari pengambilan gambar yang menyebabkan informasi palsu dan tidak relevan. Arti asli dari "noise" adalah "sinyal yang tidak diinginkan"; Fluktuasi sinyal yang tidak diinginkan pada sinyal yang diterima Oleh radio AM menyebabkan audible *acoustic noise* ("statis"). (Jayant s. Rohankar, 2013)**.** Berikut ini adalah beberapa jenis dari *image noise:*

1. *Salt and paper*

Seperti namanya *noise* jenis ini terlihat seperti garam dan lada hitam (*salt and paper*). Pada citra akan nampak seperti titik-titik. Untuk citra RGB titik-titik muncul dalam tiga warna yakni merah, hijau, dan biru. Sedangkan pada citra grayscale, noise akan muncul dalam dua warna yaitu hitam dan putih. Noise ini akan memberikan efek “on dan off “ pada pixel. Pada matlab kita akan mengatur konstanta noise. Konstanta merupakan angka numeric non negatif dengan range dari 0 sampai 1. Semakin besar konstanta noise dari citra maka citranya akan semakin kabur, sebaliknya semakin kecil konstanta efek pada citra semakin tidak terlihat. Nilai deafult untuk konstanta noise adlah 0,05.

2. *Gaissian*

Disebut juga *gaussian white noise.* Untuk menambahkan *noise* ini pada matlab memerlukan input tambahan berupa

rata-rata dan variasi. Rata-rata dan variasi merupakan suatu konstanta real. Nilainya bisa positif maupun negatif. Mekin besar rata-rata dan variasinya maka citra akan semakin kabur, sebaliknya semakin kecil konstanta efek paada citra noise akan semakin tidak terlihat. Nilai deafult adalah 0 untuk mean dan 0,01 untuk varience. Disebut white noise karena pada saat nilai rata-rata dan variasinya besar maka citra seolah-olah hanya seperti citra putih saja.

3. ***Poisson***

   Poisson noise bukan merupakan noise buatan. *Poisson* merupakan *noise* yang ditambahkan pada citra langsung tanpa kita yang menambahkan parameter apapun, sehingga efeknya pada citra pun tetap, berbeda dengan tipe *noise* yang sudah dijelaskan sebalumnya. Pada matlab jika matriks citra adalah *double precision,* maka nilai piksel inputnya dianggap sebagai mean dari distribusi poisson dengan skala 10 ^ 12.

4. ***Speckle***

   Speckle merupakan *noise* ganda. *Noise* ini ditambahkan pada citra menggunakan pera=samaan J=I=n*I, dimana n terdistribusi random seragam dengan mean 0 dan varience V. V adalah konstanta non negative yang besarnya dapat berubah ubah. Deafult nilai untuk V adalah 0,04. Makin besar nilai V maka citra akan semakin kabur.

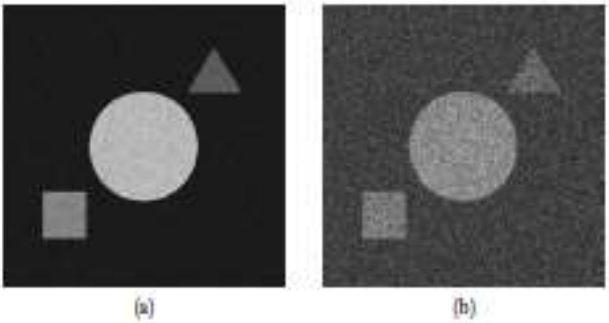
5. ***Loclvar***

   Pada matlab kita harus menggunakan dua parameter untuk menambahkan noise ini pada citra. Dua parameter tersebut berupa vektor yang ukuranya sama, dan grafik kedua parameter tersebut menggambarkan relasi fungsio-

nal antara varians noise dan intensitas citra. Vektor intensitas citra harus bernilai antara 0 sampai 1. Localvar merupakan *gaussian noise* dengan mean 0, dengan *varience noise* adalah fungsi dari intensiitas citra yang nilainya berada dalam matriks citra. Vektor intensitas citra tidak boleh bernilai sama karena citra akan nampak sebagai layar putih (*gauissian white noise*).

D. Pengaplikasian *Noise* dan *Filter* pada MRI

Noise pada citra adalah variasi nilai abu-abu yang acak, yang memberinya tampilan berbintik-bintik. Resolusi spasial dan skala abu-abu dipengaruhi oleh adanya *noise*. *Signal-to-noise Rasio* (SNR) adalah ukuran *noise* yang ada pada citra. SNR diberikan oleh sinyal rata-rata di area penting dibagi dengan standar deviasi yang diukur dari *background* citra yang terdapat *noise* . SNR memiliki citra berkualitas tinggi dimana fitur dapat dengan mudah dibedakan dari yang ada di sekitarnya.



Gambar 1.18. Ilustrasi rasio signal-to-noise (SNR) untuk gambar yang dipengaruhi oleh jumlah noise yang berbeda. (a) Citra ini memiliki sedikit noise dibanding citra lainnya. SNR untuk lingkaran besar adalah sekitar 14. (b) Dalam citra yang terdapat noise ini, SNR untuk lingkaran besar adalah sekitar 3.

Perhatikan bahwa sinyal rata-rata di lingkaran besar lebih rendah daripada yang (a), dan sinyal *background*-nya memiliki rentang nilai yang lebih besar; Keduanya berkontribusi pada pengurangan SNR. Rasio kontras-to-noise (CNR) bisa menjadi ukuran yang lebih berguna daripada SNR, karena memperhitungkan bagaimana diferensiasi jaringan dipengaruhi oleh noise. CNR diberikan oleh selisih sinyal rata-rata di dua area penting dibagi dengan standar deviasi yang diukur dari backgroung citra yang terdapat *noise.*

Rasio signal-to-noise (SNR) pada MRI: sinyal yang digunakan untuk rekonstruksi citra MR selalu rusak oleh *noise* yang disebabkan arus fluktuasi secara acak pada *receiver coil* dan objek yang dicitrakan. Kualitas citra MR dapat sangat terdegradasi oleh *noise,* sehingga sulit untuk membedakan antara struktur yang berbeda pada objek. Tiga parameter terpenting yang menentukan kualitas gambar adalah resolusi spasial, kontras gambar, dan *rasio signal-to-noise* (SNR). SNR didefinisikan sebagai rasio intensitas citra rata-rata di area penting yang dipilih (ROI) terhadap akar kuadrat variasi noise:

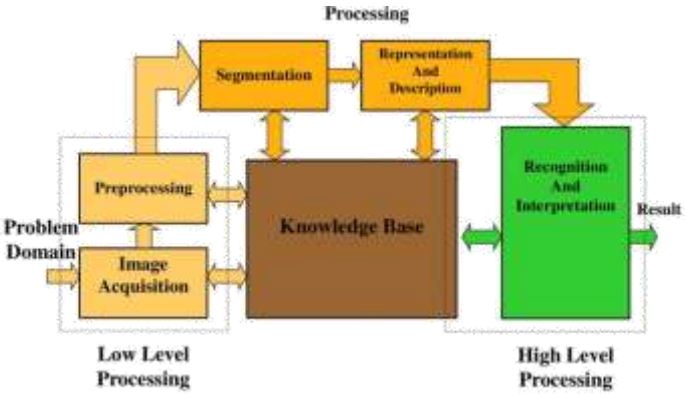
$$SNR = \frac{\text{mean intensity}}{\sqrt{noise}\ variance}$$

SNR pada MRI bergantung pada sejumlah faktor termasuk kekuatan medan magnet statis, tipe dan karakteristik r.f. coils, parameter pencitraan (misalnya, resolusi citra dan ukuran matriks), dan urutan pulsa yang dipilih. Diskusi berikut berfokus pada hubungan antara parameter SNR dan pencitraan serta kekuatan medan. Untuk diskusi tentang SNR dalam rangkaian pulsa yang berbeda dan SNR *performance* dari *r.f. coils.*

E. Teknik-Teknik Pengolahan Citra Digital

Secara umum, teknik pengolahan citra digital dibagi menjadi tiga tingkat pengolahan, yakni sebagai berikut:

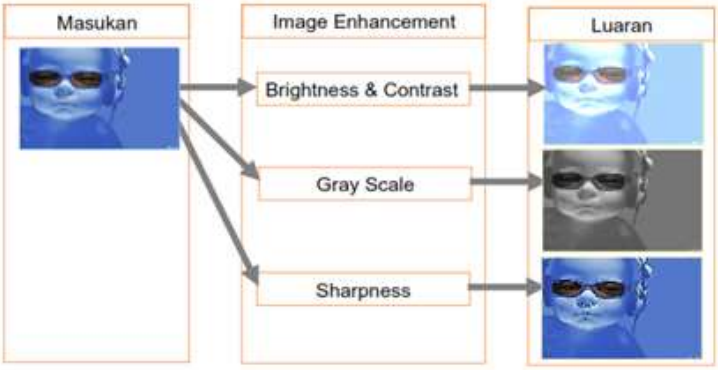
1. Pengolahan tingkat rendah *(low-level processing).* Pengolahan ini merupakan operasional-operasional dasar dalam pengolahan citra, seperti pengurangan *noise (noise reduction),* perbaikan citra *(image enhancement)* dan restorasi citra *(image restoration).*
2. Pengolahan tingkat menengah *(mid-level processing).* Pengolahan ini meliputi segmentasi pada citra, deskripsi objek, dan klasifikasi objek secara terpisah.
3. Pengolahan tingkat tinggi *(high-level processing).* Pengolahan ini meliputi analisis citra.



Gambar 1.19. Teknik-Teknik Pengolahan Citra Digital

Dari ketiga tahap pengolahan citra digital di atas, dapat dinyatakan suatu gambaran mengenai teknik-teknik pengolahan citra digital dan macam-macamnya, antara lain sebagai berikut (Basuki, 2005:11):

1. *Image enhancement*, berupa proses perbaikan citra dengan meningkatkan kualitas citra, baik kontras maupun kecerahan.

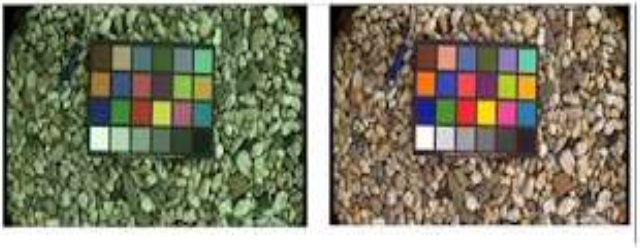


Gambar 1.20. Proses *Image Enhancement*

2. *Image restoration*, yaitu proses memperbaiki model citra,biasanya berhubungan dengan bentuk citra yang sesuai.

Gambar 1.21. Proses *Image Restoration*

3. *Color image processing*, yaitu suatu proses yang melibatkan citra berwarna, baik berupa *image enhancement*, *image restoration*, atau yang lainnya.

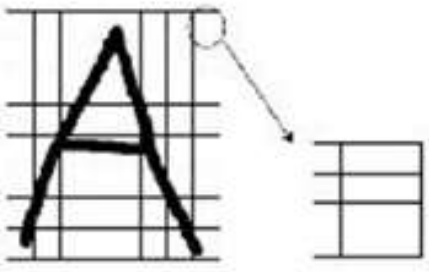


Gambar 1.22. Proses *Color Image Processing*

4. *Wavelet dan multiresolution processing*, merupakan suatu proses yang menyatakan citra dalam beberapa resolusi.

Gambar 1.23. Proses *Wavelet* dan *Multiresolution Processing*

5. *Image compression*, merupakan proses yang digunakan untuk mengubah ukuran data pada citra.



Gambar 1.24. Proses *Image Compression*

6. *Morphological processing*, yaitu proses untuk memperoleh informasi yang menyatakan deskripsi dari suatu bentuk pada citra.

Gambar 1.25. Proses *Morphological Processing*

7. *Segmentation*, merupakan proses untuk membedakan atau memisahkan objek-objek yang ada dalam suatu citra, seperti memisahkan objek dengan latar belakangnya.

Gambar 1.26. Proses Segmentasi

8. *Object recognition*, yaitu suatu proses yang dilakukan untuk mengenali objek-objek apa saja yang ada dalam suatu citra.

Gambar 1.27. Proses *Object Recognition*

F. Penerapan Pengolahan Citra Digital

a. Film

a. Menghaluskan gambar,
b. Menajamkan gambar,
c. Memberi efek terang, gelap,
d. Memberi kesan timbul,
e. Efek *morphing*, dsb.

b. Fotografi

a. Fotografi,
b. Membuat film hitam putih,
c. Memberi efek-efek seperti berkabut, cahaya,
d. Menghilangkan *noise,* dsb.

c. Kedokteran

a. Memperjelas hasil x-ray organ tubuh manusia.
b. Pengolahan citra hasil CT Scan.

d. Dunia komunikasi

a. Memperjelas foto permukaan bumi yang dihasilkan dari satelit cuaca ataupun,
b. Memperjelas foto planet-planet lain dari satelit penelitian.

e. Keamanan Data dan Proteksi hak cipta

a. Steganografi
b. Watermark

f. Pengenalan Pola

a. pola huruf
b. wajah
c. sidik jari
d. iris mata
e. tanda tangan
f. retina mata
g. suara
h. cara pengetikan
i. DNA

02 Pengertian Teknologi Biometrik

A. Konsep Sistem Biometrik

Biometriks *authentification* dalam *security* adalah hal yang sangat penting untuk menjaga keamanan data, namun sudah banyak teknologi yang diterapkan untuk mejaga keautentikan tersebut, akan tetapi hal itu banyak kendala dalam penerapannya dan masih kurang memberikan perlindungan yang aman. Teknologi biometrik menawarkan autentikasi secara biologis memungkinkan sistem dapat mengenali penggunannya lebih tepat. Terdapat beberapa metode di antaranya: *fingerprint scanning, retina scanning*, dan *DNA scanning*. Dua metode terakhir masih dalam taraf penelitian, sedangkan *fingerprint scanning* saat ini telah digunakan secara luas dan digunakan bersama-sama dengan *smartcard* dalam proses autentikasi.

Biometriks secara teoritis dapat lebih efektif untuk mengindentifikasi pribadi seseorang karena biomatriks mengukur karakteristik masing-masing pribadi untuk membedakan setiap orang. Tidak seperti dengan metoda identifikasi konvensional yang menggunakan sesuatu yang anda punyai, misalnya kartu indentitas untuk akses masuk ke suatu bangunan, atau suatu yang anda ketahui, seperti password untuk login ke sistem komputer dan lain-lain. Ketika digunakan untuk indentifikasi pribadi, teknologi biometriks

mengukur dan menganalisa karakteristik tingkah laku dan fisiologis manusia. Mengindentifikasi karakteristik fisiologis seseorang yang didasarkan pada pengukuran langsung bagian dari *body–fingertips, hand geometry, facial geometry* dan *eye retinas* serta *irises.*

Biometrik merupakan pengembangan dari metode dasar identifikasi dengan menggunakan karakteristik alami manusia sebagai basisnya, telah mempunyai peran penting dalam identifikasi manusia. Biometrik mencakup karakteristik fisiologis dan karakteristik perilaku. Karakteristik fisiologis adalah ciri fisik yang relatif stabil seperti sidik jari, siluet tangan, ciri khas wajah, pola gigi, pola iris, atau retina mata, sedangkan karakteristik perilaku, memiliki basis fisiologis yang relatif stabil namun dipengaruhi kondisi psikologis yang mudah berubah seperti tanda tangan, pola ucapan, atau ritme mengetik. [7].

Dental biometric adalah salah satu cabang biometrik yang menggunakan gigi sebagai dasar identifikasi. Metode ini telah digunakan sebagai bagian utama dari ilmu forensik selama bertahun-tahun di Belanda dan Amerika Serikat.[7] Karakteristik gigi pada seseorang dapat dijadikan sebagai dasar identifikasi karena susunan gigi manusia sangat bervariasi. Sistem pengenalan gigi secara otomatis belum sepenuhnya diimplementasikan meskipun banyak manfaat yang diperoleh dengan menggunakan gigi sebagai obyek untuk identifikasi seseorang. *Dental biometric* mempunyai beberapa kelebihan jika dibandingkan dengan cabang biometrik lainnya. Gigi memiliki struktur yang kuat dan tidak mudah berubah. Identifikasi melalui citra gigi, sangat berguna untuk pelaksanaan identifikasi terhadap jasad manusia yang telah lama meninggal sehingga elemen karakteristik fisiologis yang tersisa hanya gigi.

Dekomposisi Mode Empiris (*Emphirical Mode Decomposition*) merupakan sebuah metode dekomposisi yang adaptif dengan efisiensi tinggi yang berdasarkan karakteristik dalam skala waktu. Oleh karena itu, metode EMD dapat diterapkan pada proses nonlinier dan non-stasioner.[4] Dengan kemampuan metode EMD tersebut, penulis menerapkannya sebagai metode untuk ekstraksi ciri. Untuk meningkatkan keakurasian sistem digunakan juga metode *Principal Component Analysis* (PCA) dalam ektraksi ciri. Hasil dari ekstraksi ciri tersebut kemudian diklasifikasikan menggunakan perhitungan jarak Euclidean terdekat.

B. Dasar-Dasar Teknologi Biometrik

Dalam tahap identifikasi biometrik dapat mengidentifikasi individu-individu berdasarkan perbedaan lingkup karakteristik *behaviour*/psikologi (*biometric identifier*). Hal ini dimungkinkan bahwa karakteristik psikologi/*behaviour* setiap manusia berbeda-beda. Selain itu identifier biometrik dianggap lebih reliable dibandingkan berdasarkan pemasukan token dan pengenalan *knowledge.*

Mekanisme sistem biometrik dapat digambarkan dengan beberapa fase :

1. **Fase Penggolongan *(enrollment)***

   Pada fase ini masukan akan di pindai (scan) oleh sensor biometrik, yang merupakan representasi karakteristik digital.

2. **Fase Pencocokan**

   Dalam fase ini inputan database akan dicocokkan dengan identifikasi data. Dapat dimungkinkan adanya reduksi, sehingga dihasilkan representasi digital. Hasil ini akan diproses dengan ekstraktor ciri untuk menghasilkan suatu

representasi yang ekspresif dalam bentuk *template.* Bergantung aplikasinya *template* dapat disimpan dalam database di sistem biometrik atau dapat direkam pada kartu magnetik (atau *smartcard*).

3. Fase Pengenalan

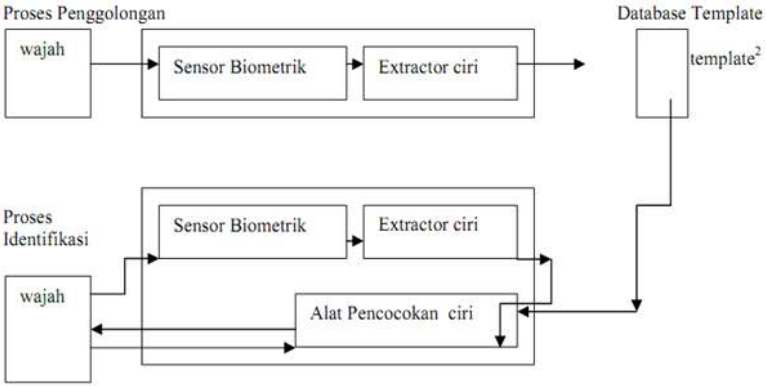
Karakteristik individu dibaca oleh pembaca biometrik (*reader*). Selanjutnya dikonversi dengan format digital, untuk diproses sebagai ekstraktor ciri (*template*). Hasil template ini selanjutnya dicocokkan dengan identifikasi individu. Lihat gambar 1.

Sistem biometrik belumlah sempurna, karena suatu saat masih dapat melakukan kesalahan dengan menerima impostor sebagai invidu yang juga valid (terjadi kesalahan pencocokan), sebaliknya terjadi penolakan terhadap individu yang valid (terjadi kesalahan ketidakcocokan). Untuk menjamin terhindarnya kesalahan seperti itu, sesuai referensi memadukan ciri biometrik wajah dengan ucapan, serta dari referensi memadukan biometrik wajah dengan ciri tanda-tangan. Selain itu dalam penerapannya ukuran database template sangatlah besar, bahkan dalam database perbankan pusat pernah terjadi bottleneck saat proses identifikasi.

Sistem biometrik yang ideal, diharapkan mempunyai karakteristik sebagai berikut:

a. Aspek universal, artinya ciri ini dapat berlaku secara umum (bahwa setiap manusia mempunyai karakteristik).
b. Aspek unik (tidak ada dua manusia yang mempunyai karakteristik yang sama).
c. Ketiga haruslah bersifat permanen (karaktristik personal yang tidak berubah-ubah) dan terakhir dapat dihim-

pun (*collectable*), karakteristik ini mudah disajikan oleh sensor dan mudah dikuantisasikan dan dikuantifikasikan.



Gambar 2.1. Mekanisme Sistem Biometrik

Selain beberapa hal yang harus diperhatikan dari mekanisme ini adalah masalah kinerja (dalam mekanisme ini akurasi sistem, kecepatan, kehandalan) perlu mempertimbangkan adanya *resource,* faktor-faktor operasional dan pengembangan, dsb. Hal ini akan berpotensi sebagai kendala teknis. Selain itu adalah akseptabilitas (daya terima pengguna) akan mendorong keyakinan *user* terhadap akurasi dan kecepatan. Serta aspek *circumvention* yaitu aspek kemudahan sistem yang tidak bergantung alat, mekanisme operasional, dsb.

Sistem *face recognition* adalah sebuah solusi identifikasi wajah dan pengenalan wajah. Sistem ini dapat diterapkan baik dalam lingkungan web maupun dalam aplikasi desktop yang menggunakan wajah sebagai autentikasinya atau pengenalan dan identifikasi wajah otomatis. Dapat berjalan

dalam lingkungan 32 bit maupun 64 bit, dapat dengan mudah diintegrasikan atau dirubah sesuai dengan kebutuhan, yang dapat memberikan keleluasaan dalam implementasi dan integrasi dengan *software* yang telah ada sebelumnya. Sistem ini dapat bekerja dengan wajah secara keseluruhan maupun dengan fitur wajah, mampu mengenali wajah dalam gambar atau foto dan *real-time video stream*, juga dapat digunakan untuk pembuatan aplikasi yang lebih luas, dari yang paling sederhana, penghilangan efek *red-eye* sampai dengan solusi login biometrik. Penerapannya bisa berupa :

1. *Real-time biometric authentication system* (sistem autentikasi biometrik secara *realtime*), yang dapat digunakan untuk login oleh user hanya dengan melihat ke arah *webcam*. Sistem ini menghilangkan autentikasi sentuhan dan *non-intrusive biometric.*
2. Tool penghilang *red-eye* otomatis yang dioptimasi dengan pengenalan fitur wajah.
3. Efek animasi wajah untuk industri *entertainment.*
4. Aplikasi image enahancement dan editor grafis.
5. Sistem otomatisasi grafis.
6. Penampil gambar, enhacers, dan pengorganisasian dengan pencarian berdasarkan wajah.
7. Aplikasi untuk kamera digital, scanner, dan webcam.
8. Tool dan plugin untuk gambar dan *video effect.*

C. Jenis-Jenis Biometrik

1. Biometrik di Bidang Kesehatan

Untuk keperluan diagnostik dan pengobatan, studi biometrik diurai menjadi. Bahan biometrik adalah bagian-bagian alat dari alat tubuh yang terlihat ataupun sensorik motorik tubuh manusia seperti: sidik jari, tulisan tangan, wajah, struktur rambut dan tulang, pigmentasi kulit, sklera mata,

motorik dan sensorik jari, dan lain sebagainya, Kode biometrik adalah tanda-tanda spesifik atau unik pada bahan-bahan biometrik seperti garis-garis pada sidik jari, warna pada sklera mata, hambatan pada sensorik motorik dan lain sebagainya, Pengindraan atau membaca kode biometrik adalah metode untuk mengenali atau menerjemahkan berbagai kode biometrik yang ada. Teknik, pembacaannya bisa menggunakan indra-indra manusia atau peralatan teknologi. Saat ini bidang kesehatan dan psikologi telah mengembangkan berbagai studi seputar membaca kode biometrik, antara lain:

a. Mengetahui struktur daya tahan tubuh (imuno) melalui lunula kuku ibu jari.
b. Mengetahui struktur ikatan batin (emo) melalui sidik jari cleft 1 dan cleft 2.
c. Mengetahui struktur alur imunitas (visera) melalui sidik jari sekitar cleft 1.
d. Memahami struktur ritme sefalografi (rileksasi dan stress) melalui cleft kapiler telapak tangan (palmar).
e. Mengetahui pola pertum-buhan tulang (osteo) melalui lingkar ibu jari dan telunjuk.
f. Mengetahui kondisi paru-paru dan nafas (pulmonal) melalui ujung jari dan kuku.
g. Mengetahui kondisi ginjal dan kandung kemih dengan lekukan jari.
h. Memahami pola pertumbuhan jaringan tubuh (plasmo) melalui grafologi lingkaran.
i. Memahami pola interaksi sosial melalui grafologi sudut kemiringan.
j. Mengetahui potensi psiko-pat dan sosiopat serta struktur *ekstra sensoric perception* (ESP) melalui sklera mata, dan lain sebagainya.

D. Proses-Proses Pengolahan Biometrik

Saat ini telah ada banyak cara untuk melakukan identifikasi manusia (*human identification*) di antaranya bisa melalui sistem biometrik. Sistem biometrik adalah identifikasi pada manusia berdasarkan karekteristik intrisik biometrik menggunakan bantuan komputer. Biometrik adalah karakteristik intrisik manusia meliputi sidik jari, wajah, iris mata, suara. Proses identifikasi manusia tanpa menggunakan sistem biometrik sering kali menimbulkan masalah diantaranya kurangnnya akurasi, lamanya proses untuk identifikasi, tidak bersifat kekal.

Beberapa contoh untuk kasus akurasi di antaranya seseorang bisa mempunyai dua kartu identitas penduduk yang berbeda. Hal ini sering ditemui karena dalam pembuatan kartu identitas tersebut tanpa dibantu dengan sistem identifikasi biometrik yang mana akan sangat sulit sekali dalam menentukan *identity* yang bersifat unik. Pencapaian dalam akurasi sebuah *identity* seseorang adalah sangat penting, yang mana hal ini bisa membantu hal pokok dalam menyelesaikan suatu masalah. Misalnya dalam investigasi kejahatan, serta untuk keamanan akses kontrol pada mesin-mesin tertentu yang bersifat krusial seperti mesin ATM. Hal tersebut sangat sulit dilakukan tanpa sistem biometrik.

Ukuran untuk sistem keamanan berbasis komputerisasi yang telah ada saat ini yaitu berdasarkan pendekatan dalam penggunaan pengetahuan atau ingatan pada manusia seperti *password, Pin* pada kartu kredit adalah metode pengamanan yang belum memberikan jaminan secara penuh, dan juga metode tersebut tidak bisa membedakan antara pemakai yang diberi hak dan seseorang yang mempunyai akses untuk *pasword atau pin* tersebut. Sistem identifikasi biometrik berdasarkan sidikjari, wajah, iris mata, suara menawarkan

sebuah identifikasi yang memberikan kelebihan dalam autentifikasi.

Aplikasi menggunakan sistem biometrik saat ini terus berkembang, hal ini dipengaruhi oleh kebutuhan akan teknologi tersebut yang semakin besar. Pada umumnya aplikasi tersebut dibagi dalam tiga kategori utama yaitu aplikasi forensik, aplikasi untuk sipil, aplikasi komersial. Beberapa contoh apliksi sistem biometrik untuk forensik yaitu identifikasi mayat, investigasi kejahatan. Aplikasi sistem biometik dalam kategori sipil bisa meliputi pembuatan kartu ijin mengemudi, pembuatan *pasport*, pembuatan kartu penduduk dan lain-lain. sedangkan untuk kategori aplikasi sistem biometrik komersial bisa meliputi akses untuk penggunaan ATM, telepon seluler, dan kartu kredit.

Gambar 2.2. Mekanisme Sistem Biometrik Iris Mata

Teknologi biometrik adalah teknologi kemanan yang menggunakan bagian tubuh sebagai identitas. Teknologi biometrik dikembangkan untuk mengatasi kelemahan penggunaan password.

1. Identifikasi dan verifikasi

Di samping itu biometrik memiliki karakteristik seperti, tidak dapat hilang, tidak dapat lupa dan tidak mudah dipalsukan karena keberadaanya melekat pada manusia, di mana satu dengan yang lain tidak akan sama.

a. *Wajah*: karena umumnya manusia mengenali seseorang berdasarkan ciri wajah.
b. *Iris*: Tekstur iris manusia berasal dari proses *chaotic morphogenetic* selama perkembangan embrio, dan memiliki ciri yang mampu dipakai untuk identifikasi seseorang
c. Suara (*voice*): memanfaatkan suara memiliki kelebihan bahwa perekaman suara seseorang tidak menyolok.
d. *Deoxyribo Nucleic Acid (DNA)*: *Deoxyribo Nucleic Acid* (DNA) adalah data berdimensi satu, yang terdiri dari sekuens basa Adenin (A), Thiamin (T), Guanin (G), dan Cytosin (C)
e. *Sidik Jari (Fingerprint* : telah diketahui bahwa sidik jari yang dimiliki seseorang berbeda dengan orang lain
f. *Telapak Tangan* : Setiap manusia memiliki pola telapak tangan yang unik. Pemeriksaan dilakukan pada guratan tangan.

Gambar 2.3. Pengenalan Wajah

a. Pengenalan Wajah

Dari berbagai metode identifikasi biometrik, pengenalan wajah adalah salah satu yang paling fleksibel. Metode ini dapat bekerja bahkan ketika subjek tidak menyadari sedang dipindai. Sistem pengenalan wajah bekerja secara sistematis dalam menganalisis karakteristik khas seseorang Teknologi pengenal wajah telah menjadi bagian dari militer dan intelijen operasi di luar negeri seperti konflik di Afghanistan dan Irak.

Teknologi ini terus berkembang hingga perangkat genggam mobile seperti tablet, *smartphone* dan bahkan kamera. Penggunaan identifikasi pengenalan wajah pada kepolisian memungkinkan penegak hukum menghentikan seorang individu hanya untuk memeriksa dan mengumpulkan gambar wajah mereka. Teknologi ini juga bisa digunakan untuk mengidentifikasi seseorang di sebuah demo politik, event olahraga atau konser musik.

Gambar 2.4. Pengenalan Sidik Jari

b. Identifikasi Sidik Jari

Sidik jari seorang manusia tidak akan pernah berubah. Identifikasi sidik jari bekerja dalam menganalisis pola dan alur-alur pada ujung jari. Penemuan POS dalam industri perdagangan secara keseluruhan adalah angin segar bagi produsen dan konsumen. Hal ini memungkinkan untuk kemudahan transaksi, kemudahan kecepatan pembayaran, dan mungkin, yang paling penting, menghilangkan kebutuhan untuk membawa uang tunai. Tetapi semua ini akan menjadi lebih baik dengan diperkenalkannya teknologi biometrik superior karena para produsen sudah mulai bereksperimen.

Bagi banyak orang, terutama di film *sci-fi* menggambarkan ide mengenai sebuah gagasan di mana pengenalan biometrik dikombinasikan dengan multi faktor authentifikasi. Pada kenyataannya, teknologi ini sudah ada dan pada tahun 2019 akan lebih berkembang karena banyak produsen sedang meningkatkan factor keamanan pada semua level teknologi, terutama di dunia usaha. Idealnya, peningkatan keamanan ini ditujukan untuk mengurangi pencurian identitas dan segala ancaman terkait dengannya. Kombinasi kata

sandi dan sidik jari (biometrik), dan mungkin komponen lain telah terbukti meningkatkan keamanan lebih dari dua kali. Pada akhirnya, bisnis mengurangi kehilangan uang untuk pencuri identitas–kerugian yang bernilai miliaran dolar secara kolektif.

Gambar 2.5. Pengenalan Sidik Jari

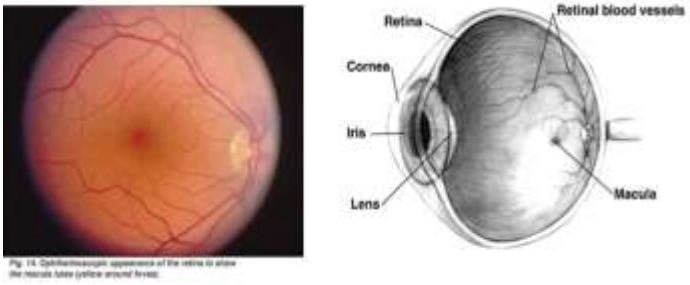
c. Pemindaian Retina

Retina seorang manusia tidak dapat ditiru oleh siapa pun. Sejauh yang diketahui, pola pembuluh darah di belakang mata berbentuk unik dan tetap sama untuk seumur hidup. pemindaian retina tetap menjadi standar dalam militer dan pemerintahan. Retina manusia adalah jaringan tipis yang terdiri dari *neuralcells* yang terletak di bagian posterior mata. Karena struktur kompleks kapiler yang memasok retina dengan darah, retina setiap orang adalah unik. Jaringan pembuluh darah di retina sangat kompleks sehingga bahkan kembar identik tidak memiliki pola yang sama. Meskipun pola retina dapat diubah dalam kasus diabetes, glaukoma atau gangguan degeneratif retina, retina biasanya tetap tidak berubah sejak lahir sampai kematian

Gambar 2.6. Pengenalan Retina Mata

d. Pemindaian Iris

Seperti retina, iris juga menyediakan data biometrik yang unik untuk ditiru. *Scanner* menggunakan sensor infrared untuk mendeteksi pola dalam iris pengguna. Cukup mengarahkannya kepada mata pengguna yang terdaftar untuk membuka ponsel, dan ia akan melakukannya dengan cepat Iris adalah lapisan di depan lensa mata berfungsi untuk mengatur lebar pupil sehingga banyaknya cahaya yang masuk ke mata dapat dikendalikan.



Gambar 2.7. Pengenalan Iris Mata

Retina Mata

Selapis tipis sel yang terletak pada bagian belakang bola mata vertebrata dan cephalopoda. Retina merupakan bagian mata yang mengubah cahaya menjadi sinyal saraf.

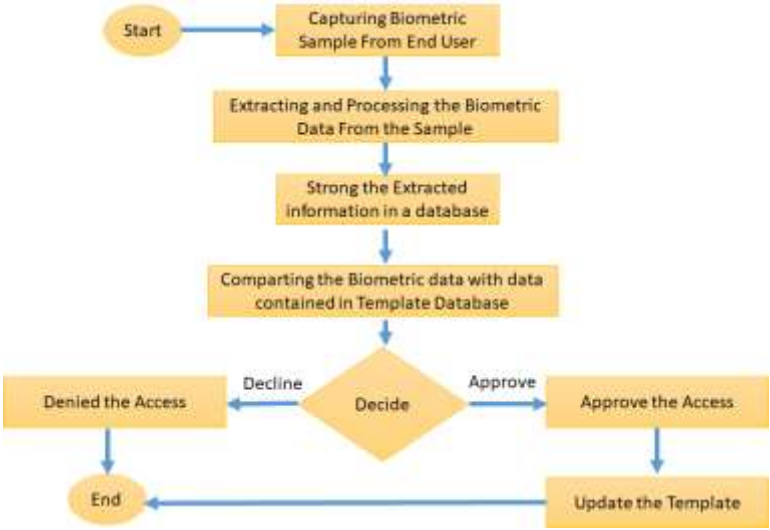
E. Metode dalam Biometrik

Berikut adalah diagram yang menggambarkan algoritma untuk *biometrics access*: Gambar 2.7 Diagram Algoritma *Biometrics Access.* Dari gambar 2.7 terlihat algoritma secara dasar bagaimana algoritma dari biometrik berjalan dalam sistem tersebut. Langkah pertama adalah melakukan input terhadap sistem biometrik sesuai dengan media yang disediakan (apabila media yang digunakan adalah *fingerprint* maka user akan memberikan sidik jadi sebagai input dalam sistem tersebut) yang kemudian dari hasil media tersebut diubah menjadi data yangdapat dibaca oleh sistem biometrik yang dapat dengan mudah membandingkan dengan sample–sample yang lain yang berperan sebagai template. Dari hasil data yang telah diubah menjadi data yang mudah dibaca tersebut disimpan kedalam database untuk menyimpan data user yang ingin memasuki sistem ini. Langkah selanjutnya adalah membandingkan data biometriks dari user dengan ada biometrik yang menjadi template pada sistem tersebut.

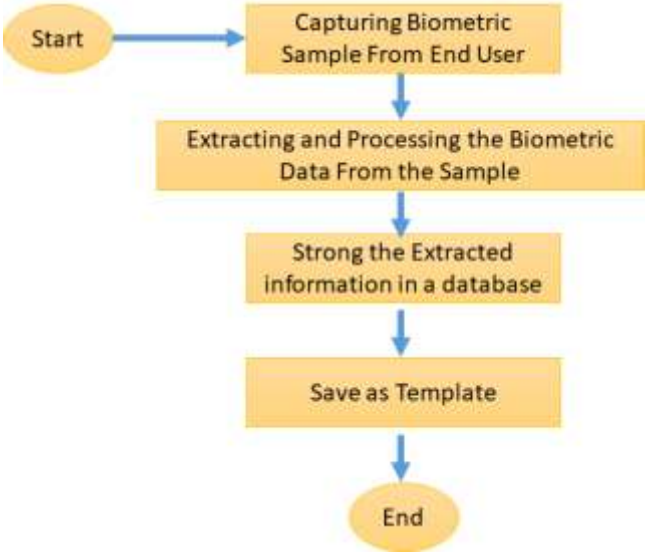
Apabila setelah dibandingkan data biometrik tersebut tidak mencapai batas persentase persamaan yang ditentukan maka user akan mengalami penolakan terhadap sistem ini, apabila sebaliknya maka user akan diterima oleh sistem dan data dari biometrik akan di-*update* sebagai data yang baru. Berikut adalah alur algoritma dari sistem biometrik untuk menentukan *template* untuk sistem. Gambar 2.8 Diagram *Algoritma Biometrics Template*. Dari Gambar 2.8 terlihat

algoritma secara dasar bagaimana algoritma dari biometrik berjalan dalam sistem tersebut untuk menyimpan sample sebagai template. Langkah pertama adalah melakukan input terhadap sistem biometrik sesuai dengan media yang disediakan (apabila media yang digunakan adalah *fingerprint* maka user akan memberikan sidik jadi sebagai input dalam sistem tersebut) yang kemudian dari hasil media tersebut diubah menjadi data yang dapat dibaca oleh sistem biometrik yang dapat dengan mudah membandingkan dengan sample–sample yang lain yang berperan sebagai *template.*

Dari hasil data yang telah diubah menjadi data yang mudah dibaca tersebut disimpan ke dalam database untuk menyimpan data user yang ingin memasuki sistem ini yang kemudian akan karakteristik metode CER faktor performa diterima oleh pengguna *fingerprint* pola pada sidik jari diterima dan dibandingkan medium kering, kebersihan dari jari tersebut medium palm scan pola dan bentuk pada telapak tangan diterima dan dibandingkan *low* cedera tangan, usia dan perhiasan *hand geometry* dimensi pada tangan dan jari dihitung dan dibandingkan *low* cedera tangan, usia dan perhiasan *high* retina pola dari pembuluh darah pada retina diterima dan dibandingkan *low* kacamata, susah digunakan *low* iris pola pada iris diterima dan dibandingkan *low* pergerakan dan pencahayaan high face bentuk pada muka diterima dan dibandingkan medium pencahayaan, kacamata, rambut, lingkungan medium *signature dynamic ritme*, kecepatan dan cara menekan diterima dan dibandingkan *high* perubahan cara tanda tangan *high keyboard dynamic* keceparan, tekanan dari kata yang menjadi kata kunci *high* perubahan cara mengetik high menjadi sebagai *template* untuk sistem tersebut.



Gambar 2.8. Diagram *Algoritma Biometrics Access*



Gambar 2.9. Diagram *Algorithm Biometric Template*

1. Tabel Biometrik

Berikut ini bagian tubuh yang saat ini dapat digunakan sebagai identifikasi untuk biometrik beserta metode, faktor yang memperngaruhi performa dan apakah diterima atau tidak biometrik tersebut (Steven M.Walker, 2002): Tabel 2.1 Tabel Biometrik.

Tabel 2.1. Karakteristik Penggunaan Biometrik oleh Pengguna

Karakteristik	Metode	CER	Faktor Performance	Diterima oleh Pengguna
Fingerprint	Pola pada sidik jari diterima dan dibandingkan	Medium	Kering, Kebersihan dari jari tersebut	Medium
Palm Scan	Pola dan bentuk pada telapak tangan diterima dan dibandingkan	Low	Cegera tangan, usia dan perhiasan	-
Hand Geometry	Dimensi pada tangan dan jari dihitung dan dibandingkan	Low	Cegera tangan, usia dan perhiasan	High
Retina	Pola dari pembuluh darah pada retina diterima dan dibandingkan	Low	Kacamata, sudah digunakan	Low
Iris	Pola pada iris diterima dan dibandingkan	Low	Pergerakan dan Pencahayaan	High
Face	Bentuk pada muka diterima dan dibandingkan	Medium	Pencahayaan, kacamata, rambut, lingkungan	Medium
Signature Dynamic	Ritme, kecepatan dan cara menekan diterima dan dibandingkan	High	Perubahan cara tanda tangan	High
Keyboard Dynamic	Kecepatan, tekanan dan kata yang menjadi kata kunci	High	Perubahan cara mengetik	High

2. Performa Biometrik

Berikut ini adalah yang digunakan sebagai matriks performa dari sistem biometrik (Donald R.Richard, 2002): *False Accept Rate or False Match Rate* (FAR or FMR): Kemungkinan untuk sistem untuk mengatakan tidak sesuai antara pola input dengan pola yang berada pada *template* yang berada pada database. FAR ini mengukur persentase dari input yang tidak valid yang tidak diterima *ÓFalse Reject Rateor False Non-Match Rate* (FRRor FNMR): Kemungkinan untuk sistem yang gagal untuk mendeteksi kecocokan antara pola input dengan *template* yang sesuai yang berada pada database. FRR ini mengukur persentase dari input yang valid tetapi ditolak oleh sistem *Receiver Operating Characteristic or Relative Operating Characte-*

ristic (ROC):Plot dari ROC merupakan karakteristik visual dari *trade-off* antara FAR dan FRR.

Secara umum algoritma pencocokan melakukan pemutusan keputusan berdasarkan batas yang menentukan seberapa mirip antara t*emplate* dan pola input dapat dibilang cocok atau *match*. Apabila batas tersebut turunkan, maka akan mengurangi *false non-match* tetapi akan meningkatkan *false accept.* Sejalan dengan itu, meningkatkan batas akan menurunkan FAR tetapi meningkatkan FRR. Variasi seperti ini disebut *Detection Error Trade-Off* (DET), yang diperoleh dengan menggunakan skala normal yang menyimpang pada kedua sumbu. Semakin linear grafik, akan semakin terlihat perbedaannya dalam performa yang tinggi *Equal Error Rate or Crossover Error Rate* (EER or CER): Tingkat di mana baik menerima dan menolak dalam jumlah yang sama. Nilai dari ERR dapat dengan mudah diperoleh dari kurva ROC.

ERR adalah cara cepat untuk membandingkan akurasi perangkat yang digunakan dengan menggunakan kurva ROC yang berbeda. Secara umum, alat yang memiliki ERR terendah merupakan yang paling akurat. *Failure To Enroll Rate* (FTEor FER): Tingkat di mana upaya untuk membuat *template* dari hasil yang diinput tidak berhasil. Hal ini sering disebabkan oleh kualitas input yang rendah. *Failure To CaptureRate* (FTC): Dalam sistem otomatis, probabilitas untuk sebuah sistem gagal untuk mendeteksi biometriks input ketika disajikan secara benar. *Template Capacity*: Jumlah maksimum dari dataset yang bisa disimpan dalam sistem.

3. Macam-Macam Biometrik

Saat ini sudah banyak sistem biometrik yang sudah digunakan. Berikut ini macam-macam biometrik yang telah diaplikasikan (V. V.Arutyunov & N. S. Natkin, 2010).

a. Biometrik dengan *Keystroke Dynamic*

Dinamika *keystroke* adalah proses menganalisis cara yang diketik oleh pengguna diterminal dengan memonitor input *keyboard* dribuan kaliper detik dalam upaya untuk mengidentifikasi pengguna berdasarkan kebiasaan pola irama mengetik. Ini memiliki sudah menunjukkan bahwa irama *keystroke* adalah tanda od melepaskan identitas. Selain itu, tidak seperti sistem biometrik lainnya yang mungkin mahal untuk melaksanakan, dinamika *keystroke* hampir gratis *hardware* yang hanya dibutuhkan adalah *keyboard.* Dinamika *keystroke* merupakan bagian dari kelas yang lebih besar dari biometrik dikenal sebagai biometrik perilaku; pola mereka adalah statistik di alam. Ini adalah kepercayaan umum bahwa biometrik perilaku yang tidak dapat diandalkan seperti biometrik fisik yang digunakan untuk otentikasi,misalnya sidik jari atau retina scan atau DNA.

Realitas di sini adalah bahwa perilaku biometrik menggunakan pengukuran kepercayaan bukanl ulus tradisional/gagal pengukuran. Dengan demikian, tolok ukur tradisional Palsu Penerimaan Rate (FAR) dan Suku Penolakan Salah (FRR) tidak lagi memiliki hubungan linier.Manfaat untuk dinamika *keystroke* (dan juga biometrik perilaku lainnya) adalah bahwa FRR/FAR dapat disesuaikan dengan mengubah ambang penerimaan pada tingkat individu. Hal ini memungkinkan untuk mitigasi risiko sesuatu secara eksplisit didefi-

nisikan individu-teknologi biometric fisik tidak pernah bisa tercapai.

Manfaat lain dari dinamika *keystroke:* mereka dapat ditangkap terus menerus- tidak hanya pada saat start-uptime-dan mungkin cukup akurat untuk memicu alarm sistem lain atau orang untuk datang memeriksa situasi.Dalam beberapa kasus,orang disenjata-point mungkin terpaksa untuk mendapatkan start-up akses dengan memasukkan passwor data memiliki sidik jari tertentu,tetapi kemudian orang bisa digantikan oleh orang lain pada *keyboard* yang mengambil alih untuk tujuan buruk. Dalam kasus lain yang kurang dramatis, dokter mungkin melanggar aturan bisnis dengan berbagi password dengan sekretarisnya, atau dengan login ke sistem medis tetapi kemudian meninggalkan komputer log-in sementara orang lain dia tahu tentang atau tidak tahu tentang menggunakan sistem. Dinamika keystroke adalah salah satu cara untuk mendeteksi masalah tersebut cukup andal untuk perlu dilakukan, karena bahkan tingkat *true-positive* 20% akan mengirimkan kata keluar bahwa jenis perilaku diawasi dan tertangkap.

b. Biometrik dengan *Facial Recognition*

Facial recognition system adalah sebuah aplikasi komputer yang digunakan untuk mengidentifikasi atau melakukan verifikasi secara langsung melalui gambar digital atau frame video. Salah satu caranya adalah dengan melakukan komparasi terhadap raut muka dari yang ada digambar dengan gambar yang ada di database (D.González Ortega,M.Martínez Zarzuela, F.J.Díaz Pernasa, J.F.Díez Higuera, M.Antón Rodríguez,

D.Boto Giralda, and J.M. Hernández Conde,2009). Teknik–teknik yang digunakan untuk melakukan *facial recognition* adalah :

1. *Traditional*, beberapa algoritma pengenalan wajah mengidentifikasi wajah dengan fitur dari gambar wajah subjek. Sebagai contoh, sebuah algoritma dapat menganalisis posisi relatif,ukuran,dan/atau bentuk mata,hidung,tulang pipi, dan rahang. Fitur-fitur ini kemudian digunakan untuk mencari gambar lain denan fitur yang cocok. Algoritma lain menormalkan galeri gambar wajah dan kemudian memampatkan data wajah, hanya menyimpan data dalam gambar yang berguna untuk deteksi wajah. Sebuah gambar probe kemudian dibandingkan dengan data wajah. Salah satu sistem yang sukses paling awal didasarkan pada teknik template yang cocok diterapkan pada satu set fitur wajah yang menonjol, menyediakan semacam representasi wajah terkompresi. Algoritma pengenalan dapat dibagi menjadi 2, yang pertama geometris dimana algoritma ini melihat dari fitur yang berbeda.Yang kedua Photometrik dimana algoritma ini melakukan pendekatan melalui statistik yang merubah gambar menjadi nilai (*value*) dan kemudian value tersebut dibandingkan dengan *template* untuk menghilangkan varian.

2. *3D Teknik 3 Dini*, menggunakan sensor 3D yang digunakan untuk menangkap informasi tentang bentuk wajah. Kemudian informasi ini digunakan untuk mengidentifikasi fitur–fitur yang berbeda pada permukaan wajah seperti kontur soket wajah hidung dan dagu. Salah satu keuntungan dari pengenalan 3D ini adalah tidak terpengaruh oleh perubahan pencahayaan. Hal ini

juga dapat mengidentifikasi wajah dari berbagai sudut padang.Kekurangan dari teknik ini adalah sensitif terhadap ekspresi dari wajah.

3. *Skin teksture analisis*, teknik yang lain adalah menggunakan rincian visual dari kulit seperti yang ditangkap melalui gambar digital atau *standart scan.* Teknik ini disebut analisis tekstur kulit. Ternyata garis–garis unik, pola dan bintik – bintik yang terlihat pada kulit dapat diubah menjadi rumus matematika.

c. Biometrik dengan *Fingerprint Recognition*

Pengenalan sidik jari atau mengacu pada metode otomatis memverifikasi perbandingan antara dua sidik jari manusia. Sidik jari adalah salah satu dari banyak bentuk biometrik digunakan untuk mengidentifikasi individu dan memverifikasi identitas mereka. Untuk biometriks ini ada dua kelas utama dari algoritma (minutia dan pola) dan empat desain sensor (optik, ultrasonik, kapasitansi pasif, dan kapasitansi aktif).

Ada beberapa pola tertentu pada sidik jari sehing-ga dapat dikenali sebuah sidik jari tersebut. 1. *Pola Arch* suatu pola di mana seperti pegunungan, masuk dari sisi kiri kemudian naik pada bagian tengah dan kelua rpada sisi kanan. 2. *Pola Loop* suatu pola di mana masuk melalui salah satu sisi jari, membentuk kurva, dan cenderung untuk keluar dari sisi yang sama mereka masuk. 3. *Pola Whorl* dalam pola ini, memiliki bentuk lingkaran (melingkar) dibagian tengah jari tersebut. Gambar 2.4 Pola Sidik Jari (dari kiri pola Arch, pola Loop, Pola Whorl).

Berikut ini adalah beberapa bentuk *minutia* yang bisa digunakan untuk mengenali sebuah sidik jari : 1.

ridge ending titik di mana *ridge* berhenti/menghilang, 2. *bifur cation* titik di mana 1 *ridge* menjadi becabang menjadi *short ridge(dot)* merupakan *ridge* yang sangat pendek dibandingkan dengan *ridge* yang biasanya. Gambar 2.4 Jenis Minutia (dari kiri *ridge ending, bifurcation, dot*) Ada beberapa sensor–sensor yang digunakan untuk mengambil sidik jari, berikut ini adalah jenis–jenis sensor yang digunakan tersebut.

1) *Optical* pencitraan sidik jari optik melibatkan menangkap gambar digital dari cetak menggunakan cahaya tampak. Jenis sensor adalah pada dasarnya, sebuah kamera digital khusus. Lapisan atas sensor, di mana jari ditempatkan, dikenal sebagai permukaan sentuh. Di bawah lapisan ini adalah lapisan pemancar cahaya fosfor yang menerangi permukaan jari. Pantulan cahaya dari jari melewati lapisan fosfor untuk sebuah *array* dari *pixel solid state* (perangkat *charge-coupled*) yang menangkap gambar visual dari sidik jari. Sebuah permukaan sentuhan tergores atau kotor dapat menyebabkan citra buruk sidik jari. Kerugian dari jenis sensor adalah kenyataan bahwa kemampuan pencitraan dipengaruhi oleh kualitas kulit pada jari. Misalnya, jari kotor atau ditandai sulit untuk gambar dengan benar. Juga, adalah mungkin bagi seorang individu untuk mengikis lapisan luar kulit pada ujung jari ketitik dimana sidik jari tidak lagi terlihat. Hal ini juga dapat mudah tertipu oleh sebuah gambar sidik jari jika tidak digabungkan dengan detektor"hidup jari". Namun,tidak seperti sensor kapasitif,sensor teknologi ini tidak rentan terhadap kerusakan elektrostatik.

2) *Ultrasonic Sensor* ultrasonik memanfaatkan prinsip-prinsi pultra sonografi medis dalam rangka untuk membuat gambar visual dari sidik jari. Tidak seperti pencitraan optik,sensor ultrasonik menggunakan gelombang suara frekuensi sangat tinggi untuk menembus lapisan epidermis kulit. Gelombang suara yang dihasilkan dengan menggunakan transduser piezoelektrik dan energi tercermin juga diukur dengan menggunakan bahan 30 piezoelektrik. Karena lapisan kulit dermal pameran karakteristik pola sidik jari yang sama,pengukuran gelombang yang dipantulkan dapat digunakan untuk membentuk sebuah gambar sidik jari. Ini menghilangkan kebutuhan untuk bersih, kulit epidermis rusak dan permukaan penginderaan bersih.
3) *Capacitance,* Kapasitansi sensor menggunakan prinsip-prinsip yang terkait dengan kapasitansi dalam rangka untuk membentuk gambar sidik jari. Dalam metode ini pencitraan, *pixel array sensor* setiap tindakan sebagai salah satu pelat kapasitor pelat sejajar,lapisan kulit (yang elektrik konduktif) bertindak sebagai piring lain, dan non-konduktif lapisan epidermis bertindak sebagai dielektrik. Pasif kapasitansi, sebuah sensor kapasitansi pasif menggunakan prinsip yang digariskan di atas untuk membentuk sebuah gambar dari pola sidik jari pada lapisan dermal kulit. Setiap *pixel sensor* digunakan untuk mengukur kapasitansi pada titik *array.* Kapasitansi bervariasi antara pegunungan dan lembah sidik jari karena fakta bahwa volume antara lapisan dermal dan elemen penginderaan di lembah berisi celah udara. Konstanta di elektrik epidermis

dan daerah dari elemen penginderaan diketahui nilai-nilai. Nilai kapasitansi diukur kemudian digunakan untuk membedakan antara pegunungan dan lembah sidik jari. Aktif kapasitansi Kapasitansi sensor aktif menggunakan siklus pengisian untuk menerapkan tegangan ke kulit sebelum pengukuran berlangsung. Penerapan tegangan kapasitor biaya yang efektif. Medan listrik antara jari dan sensor mengikuti pola dari pegunungan dilapisan dermal kulit. Pada siklus debit, tegangan melintasi lapisan dermal dan elemen penginderaan dibandingkan terhadap tegangan referensi untuk menghitung kapasitansi. Nilai jaraknya kemudian dihitung matematis, dan digunakan untuk membentuk sebuah gambar sidik jari sensor kapasitansi Aktif mengukur pola punggungan dari lapisan kulit seperti metode ultrasonik. Sekali lagi, ini menghilangkan kebutuhan untuk bersih, kulit epidermis rusak dan permukaan penginderaan bersih.

d. Biometriks dengan *Finger Vein Recognition*

Finger vein recognition adalah metode otentikasi biometrik yang menggunakan teknik pengenalan pola berdasarkan gambar pola vena jari manusia dibawah permukaan kulit.finger vein recognition adalah 32 salah satu dari banyak bentuk biometrik digunakan untuk mengidentifikasi individu dan memverifikasi identitas mereka. Jari ID Vein adalah sistem otentikasi biometrik yang sesuai dengan pola pembuluh darah di jari seseorang untuk data yang sebelumnya diperoleh. Hitachi mengembangkan dan mematenkan sistem vena jari ID pada tahun 2005. Teknologi ini sedang diguna-

kan atau pengembangan untuk berbagai macam aplikasi, termasuk otentikasi kartu kredit, keamanan mobil, waktu karyawan dan penelusuran kehadiran, otentikasi komputer dan jaringan, keamanan titik akhir dan mesin teller otomatis. Untuk mendapatkan pola untuk catatan database, individu menyisipkan jari ke terminal attester berisi dekat-infared LED (*light-emitting-diode*) cahaya dan CCD monokrom (*charge-coupled device*) kamera. Hemoglobin dalam darah menyerap dekat-infared lampu LED,yang membuat sistem vena muncul sebagai pola garis-garis gelap. Kamera merekam gambar dan data mentah digital, bersertifikat dan dikirim ke database gambar terdaftar. Untuk tujuan otentikasi, jari dipindai seperti sebelumnya dan data dikirim ke database gambar terdaftar untuk perbandingan. Proses otentikasi membutuhkan waktu kurang dari dua detik. Darah pola pembuluh yang unik untuk setiap individu, sebagaimana data biometrik lainnya seperti sidik jari atau pola iris. Tidak seperti beberapa sistem biometrik, pola pembuluh darah hampir tidak mungkin untuk palsu karena mereka terletak di bawah permukaan kulit. Sistem biometrik berdasarkan sidik jari bisa tertipu dengan boneka jari dilengkapi dengan sidik jari disalin, suara dan wajah karakteristik sistem berbasis dapat tertipu oleh rekaman dan gambar resolusi tinggi. Sistem vena jari ID jauh lebih sulit untuk menipu karena hanya dapat mengotentikasi jari dari orang hidup.

e. Biometriks dengan *Iris Recognition*

Iris recognition adalah metode otentikasi biometrik yang menggunakan teknik pengenalan pola yang didasarkan pada resolusi tinggi gambar dari iris mata individu (A. E. Hassanien,2006). Tidak menjadi bingung dengan yang lain, kurang lazim, mata berbasis teknologi, pemindaian retina. Iris *recognition* menggunakan teknologi kamera, dengan pencahayaan infra merah halus mengurangi refleksis pecular dari kornea cembung,untuk membuat gambar detail yang kaya, struktur rumit dari iris. Dikonversi ke dalam *template* digital, gambar ini menyediakan representasi matematis dari iris yang menghasilkan identifikasi positif tidak ambigu individu. Iris *recognition* keberhasilan jarang terhalang oleh kacamata atau lensa kontak. Iris teknologi telah salah satu kelompok outlier terkecil (mereka yang tidak dapat menggunakan/mendaftarkan diri) dari setiap teknologi biometrik.

Keuntungan utama dari pengenalan iris adalah stabilitas, atau umur panjang template, seperti, pembatasan trauma, sebuah pendaftaran tunggal dapat berlangsung seumur hidup. Terobosan bekerja untuk menciptakan pengenalan iris-algoritma yang diperlukan untuk akuisisi citra dan satu ke banyak pencocokan dirintis pada awal 2000-an oleh JohnG. Daugman, Ph.D, OBE (Universitas Cambridge Laboratorium Komputer) (John Daugman, 2007). Ini digunakan untuk secara efektif memulai debut komersialisasi eknologi dalam hubungannya dengan versi awal dari sistem *iris access* dirancang dan diproduksi oleh Korea LG Electronics.

Daugman algoritma adalah dasar dari hampir semua saat ini komersial dikerahkan sistem pengenalan iris. (Dalam tes dimana batas yang cocok-untuk lebih baik banding-berubah dari pengaturan default mereka untuk memungkinkan tingkat palsu-menerima di wilayah 10-410-3 untuk, iris code palsu-menolak tarif yang sebanding dengan tunggal yang paling akurat matchers-jari sidik jari.) Iris *recognition* ini memiliki cara kerja, Sebuah algoritma pengenalan iris-pertama untuk mengidentifikasi batas-batas terluar sekitar konsentris melingkar dari iris dan pupil dalam foto mata. Himpunan piksel hanya mencakup iris kemudian berubah menjadi pola bit yang melindungi informasi yang sangat penting untuk perbandingan statistik bermakna antara dua gambar iris. Metode matematis yang digunakan mirip dengan modern algoritma kompresi lossy untuk gambar fotografi.

Dalam kasus algoritma Daugman, sebuah Gabor wavelet transform digunakan untuk mengekstrak rentang frekuensi spasial yang berisi paling baik sinyal-to-noise rasio mempertimbangkan kualitas kamera yang tersedia fokus. Hasilnya adalah suatu himpunan bilangan kompleks yang membawa amplitudo lokal dan informasi fase untuk gambar iris. Dalam algoritma Daugman, semua informasi amplitudo dibuang, dan 2048 yang dihasilkan bit yang mewakili suatu iris hanya terdiri dari bit tanda kompleks representasi Gabor-domain dari gambar iris. Membuang informasi amplitudo memastikan bahwa template tetap sebagian besar tidak terpengaruh oleh perubahan dalam pencahayaan dan hampir diabaikan oleh iris warna, yang membe-

rikan kontribusi signifikan terhadap stabilitas jangka panjang dari *template* biometrik.

Untuk mengotentikasi melalui *identify* (pencocokan template yang satu-ke-banyak) atau verifikasi (satu-ke-satu pencocokan *template*), *template* yang dibuat oleh pencitraan iris dibandingkan dengan *template* nilai yang disimpan dalam database. Jika jarak Hamming berada di bawah ambang batas keputusan, identifikasi positif telah efektif telah dibuat. Masalah praktis dari pengenalan iris adalah bahwa biasanya sebagian tertutup oleh kelopak mata dan bulu mata. Untuk mengurangi FRR dalam kasus tersebut, algoritma tambahan diperlukan untuk mengidentifikasi lokasi dari kelopak mata dan bulu mata dan untuk mengecualikan bit dalam kode yang dihasilkan dari operasi perbandingan.

03 Penerapan Metode Biometrik

Teknologi biometrik (sidik jari, iris mata, profil muka) merupakan kunci utama dalam menentukan ketunggalan identitas kependudukan yang didasarkan pada keunikan informasi biometrik seseorang. Di sisi lain, saat ini belum ada industri dalam negeri yang mampu memasok teknologi biometrik untuk keperluan identifikasi maupun verifikasi berbasis sidik jari dan iris berskala besar, seperti yang digunakan dalam program e-KTP. Oleh karena itu, BPPT diharapkan berperan sebagai institusi litbangyasa pemerintah yang melakukan penguasaan teknologi melalui transfer teknologi dari luar negeri ke pelaku teknologi di dalam negeri, mendorong pengembangan dan perekayasaan teknologi biometrik baik di kalangan akademisi maupun industri. Biometrik menggantikan otentikasi metode lama dengan standar baru.

Otentikasi metode lama seperti *knowledge-based authentication* (KBA) dan SMS berdasarkan dua faktor otentikasi, seringkali digunakan di lingkungan finansial dan aplikasi perusahaan fintech tidak lagi didukung oleh National Institute of Standards and Technology (NIST). Sayangnya SMS berisi kode akses pelanggan untuk masuk ke dalam akun, terlalu mudah disusupi melalui *man in the middle* yang dipicu melalui *malware* seluler.

Adanya angka pelanggaran data profil yang tinggi dalam beberapa tahun terakhir (contoh: Equifax dan Facebook) menyebabkan keamanan berbasis KBA semakin riskan. *Personally identifiable information* (PII) saat ini bahkan dapat dibeli oleh penipu dalam website gelap. Informasi inilah yang diambil oleh penipu dari proses KBA. Fakta bahwa otentikasi ini tidak lagi aman digunakan mendorong pertumbuhan pasar otentikasi biometrik. Data dari McKinsey memperkirakan bahwa di tahun 2022, layanan verifikasi identitas akan bertumbuh hingga mencapai $20 miliar. Penerapan teknologi verifikasi identitas berbasis biometrik dapat menjadi cara cara untuk mencegah adanya penipuan. Hal ini dilakukan dengan memastikan bahwa identitas digital seseorang cocok dengan identitas fisik.

Fitur biometrik yang ditangkap dalam swafoto dibandingkan dengan ID yang dikeluarkan pemerintah. Bahkan jika ingin mengambil langkah lebih jauh saat ini telah ada teknologi *liveness detection* dan *3D liveness detection* untuk memastikan pengguna hadir secara fisik dan tidak dipalsukan (menggunakan foto, video, atau pengganti lain untuk wajah orang yang berwenang). Verifikasi ini mengharuskan pengguna untuk mengambil swafoto. Biometrik menghadirkan penggunaan tanpa hambatan permintaan konsumen untuk dapat mengakses online secara mudah semakin tinggi. Penelitian menunjukkan bahwa 93 persen konsumen lebih senang menggunakan biometrik daripada kata sandi. Biometrik menawarkan kenyamanan bagi konsumen dan lembaga keuangan yang tidak memberikan pengalaman yang sama dapat mengalami kerugian yang signifikan.

Dalam data Javelin Research dijelaskan bahwa generasi milenium, sebanyak 38 % generasi yang paling aktif menggunakan *mobile banking*, akan dengan cepat meninggalkan

mobile banking jika proses verifikasi terlalu lama. Otentikasi biometrik lebih dapat dipercaya daripada metode otentikasi tradisional. Tidak hanya karena lebih cepat namun otentikasi biometrik lebih mudah, dan lebih intuitif dalam membantu menciptakan pengalaman orientasi yang lebih baik bagi pelanggan baru.

A. Bidang-Bidang yang Menggunakan Teknologi Biometrik

Kemajuan teknologi yang semakin canggih kini memungkinkan kita untuk memiliki sistem kemanan yang lebih baik seperti password dan PIN. Namun, metode seperti ini ternyata memiliki beberapa kelemahan vital seperti mudah dipalsukan, hilang, dan bahkan mungkin tak jarang kita bisa lupa. Mengatasi celah tersebut, akhirnya ditemukanlah metode baru yang lebih akurat dan aman menggunakan identifikasi biometrik. Metode ini menggunakan bagian tubuh tertentu seperti sidik jari, suara dan iris mata untuk mengenali identitas seseorang. Teknologi biometrik hampir bisa dipastikan akan sulit di tiru karena sifatnya yang sangat unik bagi setiap orang. Banyak orang mengatakan bahwa teknologi biometrik merupakan teknologi keamanan masa depan, bahkan kini tak sedikit berbagai sektor di dunia yang telah berinvestasi dalam pengembangan teknologi biometrik untuk keperluan mereka sendiri. Ada 10 macam pengembangan teknologi biometrik yang diadaptasi baik dalam dunia kerja dan hal lainnya:

1. Personalisasi dan Keamanan Otomotif

Pasar global biometrik untuk sektor otomotif diprediksi sedang merangkak naik hingga empat tahun mendatang, dengan pabrikan seperti BMW, Audi, Mercedes-Benz dan Volkswagen semuanya telah berlomba-lomba menginteg-rasikan teknologi biometrik kedalam kendaraan mereka.

Variasi metode yang digunakan mulai dari sidik jari, pengenalan suara, dan iris mata. Untuk membuka pintu mobil hanya dengan menempelkan jari Anda, atau akses kendaraan seperti menyalakan mesin.

2. Identifikasi Penegakan Hukum

Metode pengenalan kriminal menggunakan sidik jari memang bukan hal baru, namun dengan teknologi yang semakin canggih ini, aparat hukum seperti polisi bisa lebih terbantu dalam mengenali pelaku kejahatan menggunakan scan biometrik yang terintegrasi dengan data penduduk setempat. Metode *scanning*-nya bisa menggunakan infra-merah pada sidik jari yang tertinggal di tempat kejadian perkara.

3. Layanan Finansial

Meningkatnya kejahatan *cyber* secara finansial, membuat industri finansial mau tak mau harus meningkatkan sistem keamanan dalam hal otentikasi pengguna atau nasabah. Teknologi biometrik tak hanya digunakan oleh bank di negara seperti Brazil, India, Polandia, dan Jepang untuk meningkatkan keamanan ATM, namun kini mereka juga telah menerapkan metode otentikasi suara untuk memeriksa nasabah pada awal percakapan. Bahkan yang lebih keren, sebuah bank asal UK, Halifax, kini menggunakan aksesoris khusus untuk mendeteksi detak jantung nasabah untuk membuktikan identitas mereka.

4. Travel

Menurut laporan yang dipublikasikan oleh Marketsand Markets, sektor imigrasi dan travel memegang saham terbanyak untuk pasar sistem biometrik pada tahun 2015,

diperkirakan berharga USD 32.73 milyar pada tahun 2022. Teknologi sidik jari telah umum digunakan untuk verifikasi e-paspor, e-visa, dan SIM. Negara seperti Australia bahkan telah mengumumkan rencananya untuk memberlakukan "*Contactless traveler clearance process*" untuk mencegah aktivitas kriminal dan terorisme dan mengetahui mana orang-orang yang memang benar ingin sekedar melancong.

5. **Kesehatan**
   Implementasi teknologi biometrik pada sektor kesehatan diperkirakan telah mencapai USD 2,848.3 juta pada tahun 2021. Meningkatnya penipuan kesehatan serta pencurian identitas medikal menjadi pencetus solusi biometrik. Teknologi biometrik untuk kesehatan biasanya digunakan untuk memverifikasi identitas pasien dan staff, juga akan digukan untuk proteksi terhadap penipuan dan mencegah duplikasi rekam jejak pasien, serta untuk akses kontrol pintu pada area sensitif khusus di rumah sakit dan manajemen.

6. **Keamanan Wilayah**
   Negara seperti Amerika, Amerika Latin, Eropa Timur, dan Asia telah meningkatkan keamanan dalam identikasi penduduk asing untuk mengamankan daerah perbatasan juga untuk mencegah masuknya pendatang dengan resiko kesehatan dan keamanan, atau yang menggunakan visa palsu dan kadaluwarsa. Malaysia baru-baru ini mengumumkan bahwa pekerja asing harus memiliki rekaman sidik jari di bawah pengawasan sistem biometrik negara sebelum mendapatkan visa kerja. Hal ini merupakan bentuk proteksi setelah kasus di mana pekerja mengguna-

kan kartu identitas penduduk lain untuk mendapatkan fasilitas kesehatan.

7. Komputasi

Biometrik dalam komputasi merupakan tren yang berkembang pesat. Lihat saja raksasa komputer seperti Sony, Dell, Fujitsu, HP, dan Toshiba telah mengintegrasikan teknologi biometrik pada beberapa model laptop mereka, serta raksasa *smartphon*e seperti Apple dan Samsung yang menggebrak dunia gadget dengan membawa pemindai sidik jari pada ponsel pintar besutan mereka. Banyak manufaktur yang menambahkan otentikasi biometrik untuk perangkat konsumer sebagai fitur keamanan tambahan. Pada skala yang lebih kompleks untuk keamanan organisasional, teknologi biometrik juga digunakan untuk mengamankan *user operations* dan jaringan komputer.

8. Tempat Kerja

Dari mengurangi risiko keamanan untuk penipuan jam kerja karyawan, penggunaan biometrik pada dunia kerja meliputi banyak manfaat. Mulai dari sistem absensi karyawan yang menggunakan sidik jari, yang juga dapat dikembangkan menjadi akses kontrol pintu untuk ruangan khusus dengan akses terbatas. Perusahaan modern lebih banyak memilih teknologi biometrik selain untuk keamanan dan kemudahan organisir karyawan, juga dapat diintegrasikan dengan sistem personalia yang berisi perhitungan gaji karyawan berdasarkan sistem absensi yang ada.

9. Hotel

Saat ini rata-rata hotel sudah mulai beralih menggunakan biometrik untuk memudahkan transaksi dengan para tamu dengan keamanan data yang lebih terjamin. Contohnya, banyak hotel telah mengganti sistem kartu elektronik dengan sistem kunci pintu sidik jari untuk tiap kamarnya. Tamu yang akan *check-in* melakukan scan sidik jari pada counter dan data reservasi mereka akan muncul lengkap dengan informasi pilihan mereka. Beberapa sistem tertentu memungkinkan tamu untuk mengotentikasi transaksi dan layanan menggunakan sidik jari yang akan terakumulasi dan terintegrasi langsung dengan total tagihan tamu.

10. Studi Klinis

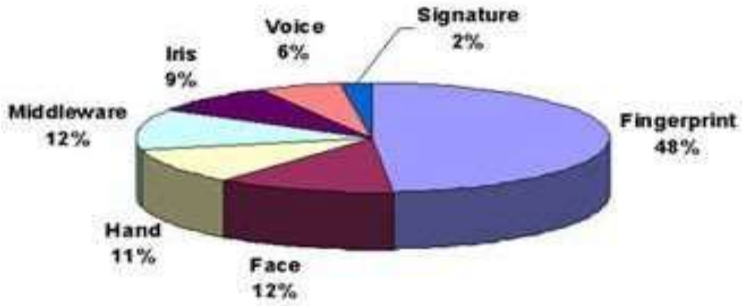
Studi klinis yang mendalami riset tertentu, teknologi biometrik digunakan untuk memastikan bahwa partisipan tersebut hanya mengikuti satu riset dalam satu waktu. Risetnya bisa bermacam-macam, seperti riset lingkungan, sosial, maupun kesehatan. Pengembangan teknologi biometrik untuk saat ini memang sedang naik daun. Di Indonesia sendiri pun penggunaannya bisa dibilang masih terbatas, masih banyak yang bisa dikembangkan lagi dari teknologi ini. Tapi paling tidak yang saat ini paling umum dipakai adalah untuk absen sidik jari di perkantoran.

B. Biometrik untuk keamanan

Teknologi biometrik merupakan teknologi yang digunakan untuk menunjukkan keaslian *(authentication)* dari individu yang melakukan akses terhadap aset organisasi. *Authentication* adalah konsep yang menunjukkan bahwa hanya mereka

yang diizinkan saja *(authentic)* yang dapat mempunyai akses terhadap asset organisasi. Biometrik bukan hanya digunakan dalam sistem informasi akuntansi, aplikasinya cukup luas. Menurut prediksi yang dilakukan oleh International Biometric Group, bahwa industri keamanan biometrik mendapat peningkatan pemasukan yang cukup besar pada tahun 2007 jika dibandingkan tahun 2003.

Implementasi *biometric security* juga dilakukan oleh pemerintah Singapura, yang saat ini sedang merencanakan penggunaan paspor biometrik pada Oktober 2005 dan saat ini 9000 penduduk Singapura yang bekerja di *airlines* telah bersedia untuk melakukan uji coba paspor biometrik selama 6 bulan. Paspor ini memuat data-data pribadi pemiliknya, seperti bentuk muka, sidik jari, dan bahkan pola selaput pelangi mata atau iris. Semua data ini, akan disimpan dalam sebuah *chip* memori yang termuat dalam paspor biometrik. Hal yang lebih menarik lagi adalah ketika para pemilik paspor lama tidak perlu mengganti jika paspor tersebut sudah kadaluarsa, yang perlu dilakukan hanya menambahkan chip ini ke dalam paspor yang sekarang dimiliki. Penggunaan paspor teknologi biometrik ini dilakukan oleh Pemerintah Singapura sebagai respon untuk meningkatkan keamanan dalam negeri (Radio Singapore International 2004). Kondisi ini bukan hanya terjadi di Singapura, IBM sebagai industri yang bergerak dalam bidang produsen notebook juga berencana akan menerapkan teknologi biometrik sebagai salah satu pengamanan *notebook* terbaru (*notebook thinkpad*) yang akan dikeluarkan oleh perusahaan ini (SPI 18: 2005).



Gambar 3.1. Penyebaran Pendapatan di antara *Biometric Security* (Sumber: International Biometric Group 2004)

Penerapan teknologi biometrik ini ternyata juga bukan hanya digunakan di luar negeri, di Indonesia ternyata fenomena ini sudah kelihatan, contohnya PT Legoso Securinfo dan juga PT. DataSript yang sudah menawarkan penerapan teknologi biometrik pada sistem absensi, dengan menggunakan *fingerprint*. Hal ini juga diikuti dengan munculnya tas biometric yang dirancang oleh Universitas Indonesia khusus untuk tas wanita (jawapos.com). Pembahasan dalam tulisan ini akan diarahkan pada elemen *security*, sebagai salah satu elemen yang harus dimiliki oleh sebuah sistem yang *reliable.* Dalam pendekatan *security* ini akan diperkenalkan teknologi biometrik, sebagai alternatif teknologi yang dapat digunakan sebagai pengendalian dalam sebuah sistem informasi akuntansi.

Sistem informasi akuntansi yang terkomputerisasi, tentu saja tidak bisa dilepaskan dari aspek teknologi informasi yang mempengaruhi sistem informasi akuntansi. Sistem informasi akuntansi yang terkomputerisasi semakin banyak digunakan pada kondisi sekarang karena biaya *hardware* dan *software* yang sudah mulai dapat dijangkau oleh organisasi,

bahkan sistem informasi akuntansi yang terkomputerisasi juga dapat diperoleh melalui *web browser*. Sistem informasi akuntansi yang berbasis web, seperti yang ditawarkan oleh NetLedger dapat diakses dari seluruh dunia.

Tiga keuntungan sistem informasi akuntansi yang terkomputerisasi dibandingkan sistem manual (Warren 2005: 250), yaitu (1) Menyederhanakan proses pencatatan dan penyimpanan data. Transasksi dicatat secara elektronik dan pada waktu bersamaan diposting secara elektronik ke buku besar dan buku besar pembantu (2) Sistem komputerisasi biasanya lebih akurat dibandingkan sistem manual (3) Sistem komputeriasi menyediakan informasi bagi manajemen dengan informasi saldo akun yang realtime, hal ini disebabkan *posting* yang dilakukan secara langsung dari jurnal ke buku besar pada saat yang bersamaan.

Pengendalian yang dibutuhkan pada kondisi sistem informasi akuntansi terkomputerisasi tentu saja akan berbeda dengan sistem informasi akuntansi manual, sehingga dalam konteks sistem informasi akuntansi yang berbantuan teknologi juga akan membutuhkan pengendalian yang berbantuan teknologi. Dalam memenuhi kebutuhan ini, maka teknologi *biometric security* merupakan alternatif yang dapat dipertimbangkan dalam pengendalian sistem informasi akuntansi yang terkomputerisasi. Teknologi *biometric security* merupakan pengendalian yang dibutuhkan dalam sistem informasi terkomputerisasi, dalam konteks menentukan *authentication.* Konsep *something you are* yang dikembangkan menjadi teknologi biometrik merupakan model *authentication* yang paling akurat dibandingkan kedua model *authentication* yang ada. (Chandra and Calderon 2003:54).

Organisasi profesi dalam bidang akuntansi sebenarnya telah banyak memberikan kontribusi dalam memunculkan ide

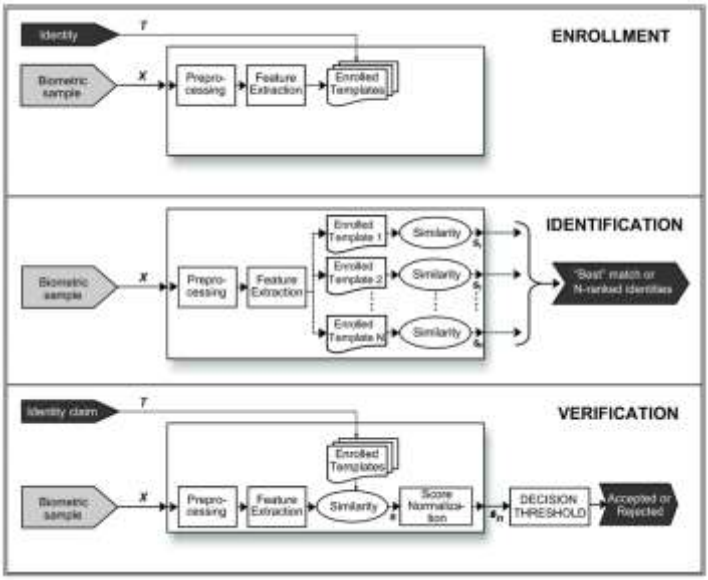
terhadap kerangka dan standar yang berkenaan dengan pengendalian dalam suatu business process dan lebih khusus pada sistem informasi akuntansi. Struktur Pengendalian Internal (SPI) yang terdiri dari lima komponen pengendalian yang ada sekarang, merupakan hasil pengembangan yang dilakukan oleh COSO (Committee of Sponsoring Organizations) yang merupakan aliansi dari beberapa organisasi profesi akuntansi, seperti American of Accounting Association (AAA), American Institute Certified Public Accountant (AICPA), Institute of Internal Auditor (IIA), Institute of Management Accountants (IMA) dan Financial Executive Institute. Selain SPI juga dikembangkan pengendalian yang digunakan untuk sistem komputerisasi, yaitu COBIT (Control Objective for Information and Related Technology) yang dikembangkan oleh Information System Audit and Control Foundation (ISACF).

Merupakan hal yang sangat tidak mungkin jika sebuah organisasi dapat melakukan business process tanpa adanya pengendalian yang ada dalam organisasi itu sendiri. Pengendalian itu merupakan sebuah sistem yang mencegah, mendeteksi dan melakukan perbaikan terhadap tindakan yang tidak sesuai dengan hukum yang ada (Weber 1999:35). Dua hal yang perlu diperhatikan dari definisi pengendalian tersebut, yang pertama berkenaan dengan kata sistem. Pengertian dari sistem adalah, seperangkat komponen yang berelasi antara satu elemen dengan elemen yang lain untuk mencapai satu tujuan (Romney and Steinbart 2003:2). Hal yang perlu diperhatikan disini adalah password maupun teknologi *biometric security* tidak bisa dikatakan sebagai pengendalian, jika password dan teknologi *biometric security* tersebut berdiri sendiri (Weber 1999:35). Namun jika password dan teknologi *biometric security* tersebut berelasi dengan kom-

ponen yang lain untuk mencapai satu tujuan yakni mencegah, mendeteksi dan melakukan perbaikan terhadap tindakan di luar hukum, maka password dan *biometric security* dikatakan sebagai pengendalian.

Jika berbicara mengenai teknologi *biometric security* maka *biometric security* merupakan komponen *information technology infrastructure* yang berperan sebagai teknologi pendukung dalam sistem. Hal kedua yang perlu digaris bawahi berkenaan dengan pengertian pengendalian adalah kata di luar hukum. Weber (1999:35), mendefinisikan di luar hukum ini sebagai tindakan yang *unauthorized, inaccurate, incomplete, redundant, ineffective* atau *inefficiient* ketika melakukan akses terhadap aset atau fasilitas dalam organisasi.

Secara umum ada tiga model *authentication* yang digunakan dalam mengamankan aset sebuah organisasi (Liu & Silverman 2004) yaitu (1) *Something you have (possession):* kunci atau kartu identitas (2) *Something you know (knowledge):* password, PIN atau kata kunci yang digunakan untuk melakukan suatu akses ke dalam asset organisasi (3) *Something you are (biometric)*: teknologi *biometric security.* Ketiga model tersebut dapat dilihat pada gambar di bawah ini.



Gambar 3.2. *Authentication Model*
(Sumber: Chandra and Calderon 2020:54)

Weber (1999:34) membedakan antara pengendalian (*control*) dengan pengamanan (*security*) dengan baik sekali. Dijelaskan oleh Weber (1999:35) bahwa teknologi *biometric security* tidak akan dinamakan sebagai pengendalian jika teknologi *biometric security* berdiri sendiri, namun ketika teknologi *biometric security* digunakan sebagai teknologi yang mendukung dalam sistem informasi akuntansi, maka teknologi *biometric security* dinamakan sebagai salah satu pengendalian dalam sistem informasi akuntansi. Hal yang sama juga dikatakan oleh Byrne (2003:44), bahwa teknologi *biometric security* sebagai salah satu teknologi dalam *identity management* seharusnya tidak berdiri sendiri hanya sebagai teknologi sendiri, seharusnya teknologi *biometric security* merupakan salah satu komponen dalam sistem informasi akuntansi yang ada. Berdasarkan komponen sistem informasi akuntansi

maka posisi teknologi *biometric security* dalam sistem informasi akuntansi tentu saja sebagai information *technology infrastructured* (Romney and Steinbart 2003:2).

Konsep Byrne sebenarnya dapat dikembangkan menjadi suatu *integrated system*, yaitu penggunaan teknologi *biometric security* secara komprehensif dalam lingkup yang lebih besar, yakni dalam lingkup sistem informasi manajemen. Pengendalian *biometric security* digunakan untuk mendukung implementasi sistem informasi manajemen, bukan hanya pada sistem informasi akuntansi. Namun kembali lagi harus dikritisi bahwa tidak setiap organisasi akan menerapkan solusi yang sama dalam mengimplementasikan *biometric security*. Ada beberapa organisasi yang hanya menerapkan *biometric security* pada tingkat solusi sistem informasi akuntansi dan sementara organisasi yang lain langsung pada tingkat solusi manajemen.

Implementasi teknologi *biometric security* cukup luas dalam hal pengendalian dalam sistem informasi akuntansi, di antaranya: (1) *Physical access*. Penggunaaan teknologi *biometric security* sudah cukup banyak digunakan dalam hal *physical access*. Aplikasi ini digunakan dalam hal melindungi aset organisasi berupa aset fisik, baik berupa akses kedalam ruangan maupun akses kedalam aset organisasi. Penggunaan *biometric security* akan lebih optimal penggunaannya ketika digunakan untuk jumlah user yang besar. Sebagai contoh penggunaan *biometric security* untuk 65.000 orang pada Olympiade tahun 1996. Hal ini dilanjutkan oleh Disney World dengan menggunakan *fingerprint* pada sistem parkir Disney World. International Air Transport Association juga mempunyai program untuk mengimplementasikan sistem *biometric security* dalam bentuk *eye ticket*, di mana bandara

North Carolina dan Flughafen Frankfurt akan menjadi *file project* dari program ini.

Dalam penerapan untuk sistem informasi akuntansi, teknologi *biometric security* dapat digunakan untuk mencegah *inventory fraud* (Chandra and Calderon 2003:26). Kondisi ini akan memungkinkan hanya setiap individu yang sudah diotorisasi oleh sistem yang dapat mempunyai akses terhadap *inventory* yang dimiliki organisasi (2) *Virtual Access*. Weber (1999:224), membagi *information system assets* menjadi dua, yakni *physical asset* dan *logical asset*. *Virtual access* termasuk aplikasi *biometric security* untuk melindungi *logical asset* yang berupa data maupun *software*. *Virtual access* ini lebih banyak digunakan dalam menjaga keamanan data dalam jaringan.

Umumnya data yang ada dalam jaringan, dilindungi dengan menggunakan password atau PIN. PIN atau password tidak dapat menjamin akses yang dilakukan oleh individu yang di luar otorisasi karena merupakan hal yang sangat memungkinkan jika nomor PIN atau password tersebut dapat diketahui oleh individu lain. Sebagaimana dikemukakan oleh Ernst & Young, bahwa 84% dari fraud yang terjadi pada organisasi komersial, disebabkan oleh pemberitahuan password atau PIN kepada individu lain (Byrne 2003:42). Teknologi *biometric security* memungkinkan bahwa data yang ada dalam jaringan tersebut hanya diakses oleh individu-individu yang benar-benar diizinkan (*authentication*), sehingga prinsip data *integrity* dalam sistem informasi akuntansi dapat dijaga dalam konteks ini (3) *E-commerce applications*. Aplikasi teknologi *biometric security* dalam hal *e-commerce* mulai diperhitungkan oleh para ahli teknologi informasi di bidang *cybercommerce.*

Mekanisme dari aplikasi ini memang masih membutuhkan *biometric device* yang berfungsi sebagai *biometric reader*

pada setiap tempat transaksi *e-commerce*. Jika transaksi *e-commerce* dilakukan melalui rumah ataupun kantor maka kondisi ini mengharuskan adanya *biometric reader* yang dimiliki oleh individu yang melakukan transaksi *e-commerce.* Namun pada kondisi perkembangan teknologi yang demikian pesat, sangat memungkinkan penggunaan layar komputer sebagai *biometric reader,* sehingga tidak memerlukan *biometric device* yang berfungsi sebagai *biometric reader* lagi. Sebagai buktinya Nuance communication mulai mengembangkan media telepon yang berfungsi sebagai perantara *biometric reader* yang dapat digunakan ketika ingin melakukan proses *authentication* yang berupa gelombang suara pada transaksi *e-commerce*.

Implementasi *biometric security* pada *e-commerce* dilatarbelakangi karena fenomena penipuan melalui *e- commerce* menjadi sesuatu yang sangat diwaspadai oleh para pelaku yang menjual produknya melalui *on-line shopping*. Dalam konteks ini *biometric security* berperan sebagai pengendalian dalam salah satu *accounting subsystems*, yakni *revenue cycle.* Pengendalian dalam *revenue cycle* untuk *e-commerce* merupakan sesuatu yang harus menjadi prioritas bagi organisasi yang terlibat dalam *e- commerce.*

Hal ini sesuai dengan survei yang dilakukan oleh Clear Commerce yang menyatakan bahwa tingkat penipuan melalui *on-line shopping* sangat tinggi, hal ini terutama terjadi pada kondisi ketika individu-individu dari negara-negara berkembang bertindak sebagai pembeli. Survei ini juga menyatakan negara Indonesia merupakan negara kedua setelah Ukraina sebagai *country of origin* kejahatan yang menggunakan *credit card* sampai tahun 2003 (Ahmadjayadi dan Cahyana 2004). Untuk mengatasi permasalahan ini, MasterCard sedang mengembangkan implementasi teknologi *security* dalam *e-*

commerce, di mana MasterCard memperkirakan bahwa penggunaan teknologi *biometric* dalam *e-commerce* akan mengurangi penipuan hingga 80%, ditinjau dari sisi keunggulan yang dimiliki teknologi *biometric security* (Liu and Silverman 2004) (4) *Covert surveillance*. *Covert surveillance* merupakan topik yang masih jarang diteliti dan merupakan aplikasi yang sulit untuk diimplementasikan (Liu and Silverman 2004).

Hal ini dapat dipahami, karena aplikasi teknologi biometrik membutuhkan dukungan dan komitmen dari pemerintah sebagai elemen yang memegang peranan yang sangat penting dalam hal infrastruktur untuk implementasi teknologi *biometric security*, khususnya aplikasi *covert surveillance*. *Covert surveillance* digunakan pada gedung-gedung milik umum atau fasilitas-fasilitas umum yang memungkinkan semua orang melakukan akses. Tujuan dari aplikasi ini sebenarnya bukan pada proses *authentication,* namun lebih kearah proses *capturing* data atas semua individu yang melakukan akses terhadap gedung-gedung maupun fasilitas umum, sehingga proses ini memungkinkan dilakukannya pemantauan atas identitas pengunjung fasilitas milik umum, dalam hal inilah yang membuat aplikasi ini disebut sebagai *covert surveillance* atau pengamatan secara sembunyi-sembunyi.

Kemungkinan ide ini muncul, ketika serangan teroris dalam bentuk bom yang terjadi pada gedung-gedung dan fasilitas umum. Melalui teknologi *biometric security*, data dari semua pengunjung dan pengguna fasilitas dan gedung tersebut dapat dilacak secara cepat. Namun aplikasi ini juga dapat digunakan pada perusahaan-perusahaan, misalnya pada ruangan-ruangan maupun fasilitas yang ada pada perusahaan, sehingga akan diketahui semua data individu yang melakukan akses. Jika pada konsep *physical access*, teknologi biometrik

hanya berperan sebagai pengendalian, agar individu yang memiliki otorisasi saja yang mempunyai akses terhadap aset organisasi.

Teknologi *covert surveillance* memungkinkan organisasi memiliki data individu yang melakukan akses terhadap aset organisasi, sehingga dapat dilakukan pengendalian dan evaluasi atas akses individu terhadap aset organisasi. Tidak semua teknologi *biometric security* dikondisikan untuk menyimpan data individu yang melakukan proses *authentication* hal ini disesuaikan juga dengan kebutuhan organisasi. Maksudnya, kondisi ini akan berpengaruh pada kapasitas database dari teknologi *biometric security* yang akhirnya mempengaruhi sisi *cost* yang harus dikeluarkan organisasi untuk mengimplementasikan teknologi ini.

C. Pengenalan Pola

Pengenalan pola dan kaitannya dengan identifikasi biometrik menjadi sebuah ilmu yang popular dalam bidang teknologi informasi dan komunikasi. Pengenalan pola dalam identifikasi biometrik mencakup hal yang luas, meliputi pengenalan wajah, pengenalan pola sidik jari, pengenalan pola iris dan retina, pengenalan geometri tangan, pengenalan sklera mata, pengenalan pola skin mark, pengenalan pola pembuluh darah dan pengenalan pola *androgenic hair* [1-2]. Pengenalan pola biometrik bermanfaat di berbagai bidang. Pada bidang *information security*, pengenalan pola biometrik menjadi begitu penting karena bermanfaat membantu pihak berwenang dalam mengungkap identitas kriminal.

Pengenalan pola wajah dan sidik jari membantu pihak berwenang untuk dapat mengetahui identitas kriminal yang tertangkap di kamera (wajah) atau menempel di barang bukti (sidik jari) dengan membandingkannya dengan basis data

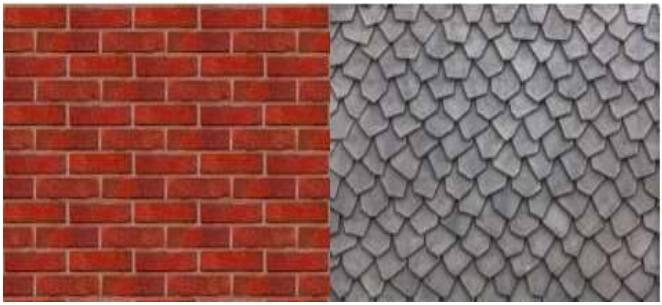
pemerintahan atau basis data kriminal. Pengenalan pola *skin mark* menjadi salah satu identifikasi biometrik yang popular sejak kesuksesannya dalam trial United States vs Michael Joseph Pepe [3-4]. Pola nevi (*skin mark*) yang terletak di paha kiri Joseph Pepe yang kemudian membuatnya terbukti bersalah dan menjadi terdakwa dari kasus pelecehan seksual anak. Pengenalan pola *skin mark* [5-7] dan *blood vessel* [8-9] mencapai perkembangan yang signifikan karena kemampuannya dalam membantu identifikasi kriminal pada kasus di mana data wajah dan bagian tubuh yang bisa diidentifikasi seperti tato tidak ada. Kekurangan pengenalan pola *skin mark* dan *blood vessel* adalah tidak *robust* jika bagian tubuh yang diidentifikasi ditumbuhi *androgenic hair*. Dari masalah ini, dikembangkanlah pengenalan pola berdasarkan pola *androgenic hair* [10-13].

Pengenalan pola dalam identifikasi biometrik membutuhkan metode pengenalan yang akurat agar tidak terjadi kesalahan dalam identifikasi. Banyak penelitian telah dilakukan berusaha untuk menganalisis metode yang terbaik untuk setiap ciri biometrik. Masing-masing biometrik tidak dapat diterapkan metode pengenalan yang sama dalam hal mencari keakuratan tertinggi. Hal ini dikarenakan setiap ciri biometrik adalah unik dan diperlukan pendekatan yang berbeda untuk masing- masing ciri biometrik. Penelitian sistem pengenalan dikembangkan dan dikerjakan dengan meneliti sistem dari berbagai perspektif. Penelitian dengan persepektif analisis dari pemilihan tahap pra proses [14], perspektif analisis dari metode ekstraksi fitur [15-17] dan dari perspektif penggunaan metode klasifikasi yang tepat untuk mencari kelompok yang paling sama antara input dan basis data [18-19]. Susunan dari paper ini adalah sebagai berikut, pada bagian 2 akan dibahas metode pra proses. Pada bagian 3 akan dibahas

metode ekstraksi fitur dan bagian 4 akan membahas metode klasifikasi. Kesimpulan akan dibahas pada bagian terakhir yaitu bagian 5.

1. Apa itu Pola (*Pattern*)

Pola adalah objek, proses, atau kejadian yang dapat diberi nama. Pola adalah himpunan pengukuran yang menggambarkan sebuah objek. Tekstur merupakan karakteristik intrinsik dari suatu citra yang terkait dengan tingkat kekasaran (*roughness*), granularitas (*granulation*), dan keteraturan (*regularity*) susunan struktural piksel. Aspek tekstural dari sebuah citra dapat dimanfaatkan sebagai dasar dari segmentasi, klasifikasi, maupun interpretasi citra. Tekstur dapat didefinisikan sebagai fungsi dari variasi spasial intensitas piksel (nilai keabuan) dalam citra. Berdasarkan strukturnya, tekstur dapat diklasifikasikan dalam dua golongan: makrostruktur dan mikrostruktur, Tekstur makrostruktur memiliki perulangan pola lokal secara periodik pada suatu daerah citra, biasanya terdapat pada pola-pola buatan manusia dan cenderung mudah untuk direpresentasikan secara matematis. Contoh tekstur makrostruktur sebagaimana pada Gambar 3.1. berikut:



Gambar 3.3. Citra tesktur makrosutruktur

Pada tekstur mikrostruktur, pola-pola lokal dan perulangan tidak terjadi begitu jelas, sehingga tidak mudah untuk memberikan definisi tekstur yang komprehensif. Gambar 3.2. berikut ini menunjukkan contoh tekstur mikrostruktur.

Gambar 3.4. Citra tekstur mikrostruktur

2. Apa itu Kelas Pola ?

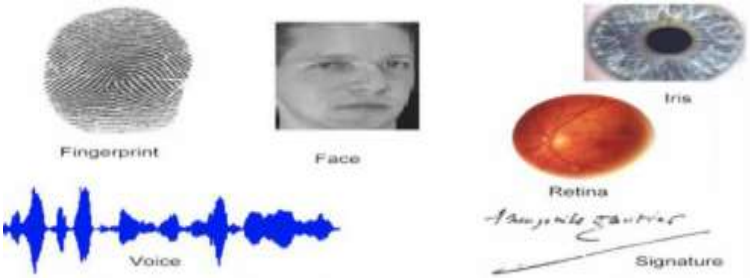
Kelas pola/kategori merupakan himpunan pola yang memiliki atribut tertentu. Kumpulan dari beberapa objek yang identik (kemiripan data). Selama proses pengenalan objek dimasukkan ke dalam kelas yang ditentukan.

Gambar 3.5. Jenis-Jenis Pola Huruf

3. Apa itu Pengenalan Pola?

Proses untuk menemukan hubungan suatu pola terhadap pola-pola sebelumnya. Belajar membedakan pola yang dianggap penting terhadap latar belakangnya. Mengguna-

kan teori, algoritma, sistem untuk meletakkan/mengelompokkan pola-pola ke dalam kategori.



Gambar 3.6. Jenis-Jenis Pola Biometrik

4. Persepsi Manusia

Manusia telah dianugerahi kemampuan untuk menerima rangsangan (indera) dari lingkungan dan memberikan aksi terhadap apa yang diamati

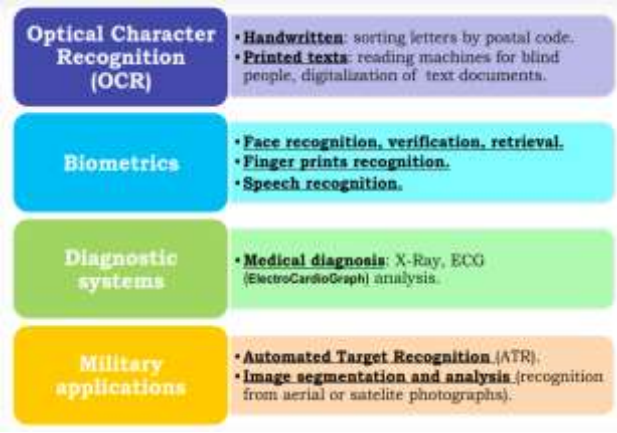
a. Mengenali wajah
b. Memahami kata yang diucapkan
c. Membaca tulisan tangan
d. Membedakan makanan segar dari baunya

Tujuan dari pengenalan pola adalah *menjadikan mesin (komputer) memiliki kemampuan yang mirip dengan manusia.*

5. Persepsi Manusia dan Mesin

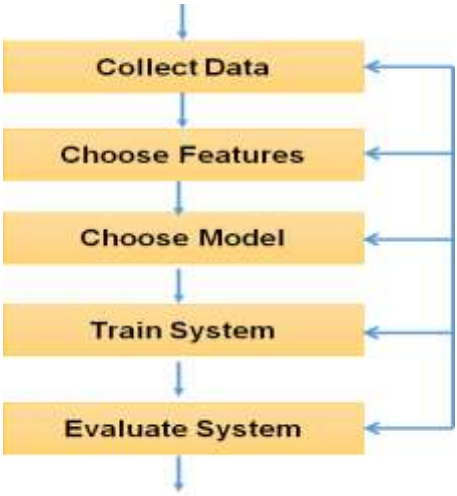
a. Kita sering dipengaruhi oleh pengetahuan tentang bagaimana pola dimodelkan dan dikenali secara alami ketika kita membangun algoritma pengenalan pola.
b. Penelitian tentang persepsi mesin juga membantu kita mendapatkan pemahaman lebih dalam dan apresiasi untuk sistem pengenalan pola secara alami.

c. Sampai saat ini, kita telah mengaplikasikan beberapa teknik yang murni secara numerik dan tidak ada korespondensinya dengan sistem alamiah.



Gambar 3.7. Contoh Aplikasi Teknologi Biometrik

D. Tahapan Pengenalan Pola



Gambar 3.8. Tahap Pengenalan Pola

1. ***Collect Data***

   Bagaimana mengetahui fitur apa yang dipilih, dan bagaimana kita memilihnya? (Misal transformasi data fitur dengan PCA). Mengambil nilai data dari objek, tipe data berdasarkan penskalaan datanya:

   a. Data Kualitatif: Data yang bukan berupa angka. Terbagi dua :
      1) Nominal: Data yang paling rendah dalam level pengukuran data. Contoh: jenis kelamin, merk mobil, nama tempat.
      2) Ordinal : Ada tingkatan data. Contoh : sangat setuju, setuju, kurang setuju, tidak setuju.

   b. Data Kuantitatif: Data berupa angka dalam arti sebenarnya. Terbagi dua :
      1) Data Interval, contoh: interval temperatur ruang adalah sebagai berikut: Cukup panas jika antara 50C-80 C, Panas jika antara 80 C-110 C, Sangat panas jika antara 110 C-140 C.
      2) Data Rasio, tingkat pengukuran paling 'tinggi'; bersifat angka dalam arti sesungguhnya. Contoh: tinggi badan, berat badan, usia.

2. ***Choose Features***

   Apa algoritme yang akan digunakan? Apakah ada algoritme yang terbaik ...?. Pemilihan fitur - feature extraction - disesuaikan dengan kasusnya.

   Object to Dataset

   a. Text
   b. Citra
   c. Audio

d. *Video*
e. *Etc*

Tabel 3.1. Karakteristik Pemilihan Features dan Class

No.	Fitur-1	Fitur-2	..	..	Fitur-N	Kelas
1						
2						
3						
...						
..						
M						

Keterangan :

a. M menyatakan banyak data, N menyatakan banyak fitur.
b. Ektraksi fitur dilakukan jika data yang diamati masih berupa data mentah (misalnya masih berupa kumpulan data awal).
c. Fitur yang diambil adalah yang merupakan ciri khas yang membedakan satu objek dengan objek lainnya.

3. *Choose Model*

Jenis teknik/pendekatan pengenalan pola.

a. *Template matching* : berdasarkan *template*
b. *Statistical:* berdasarkan model statistik dari pola dan kelas pola yang diberikan.
c. Structural (*or syntactic*): kelas pola direpresentasikan oleh struktur formal seperti grammar, string, automata, dll.
d. *Neural networks*: mesin klasifikasi yang direpresentasikan oleh model sel neuron dari otak manusia.

Tabel 3.2. Jenis Teknik/Pendekatan Pengenalan Pola

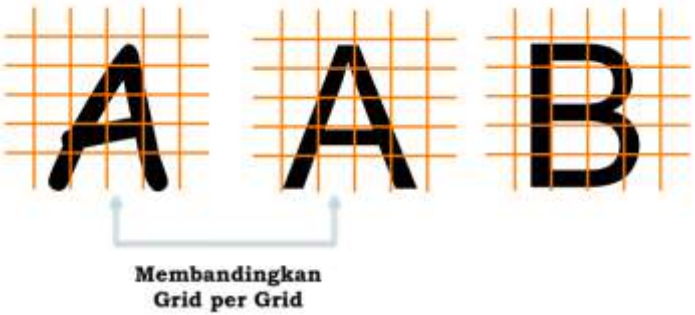
No.	Approach	Representation	Recognition Function	Typical Criterion
1	Template Matching	Sample, Pixels Curve	Correlation, Distance, Measure	Classification errors
2	Statistical	Features	Discriminant, Function	Classification errors
3	Syntactic or Structural	Primitives	Rules, Grammar	Acceptance Errors
4	Neural Network	Sample, Pixels, Features	Network, Function	Mean Square Errors

a. Template Matching

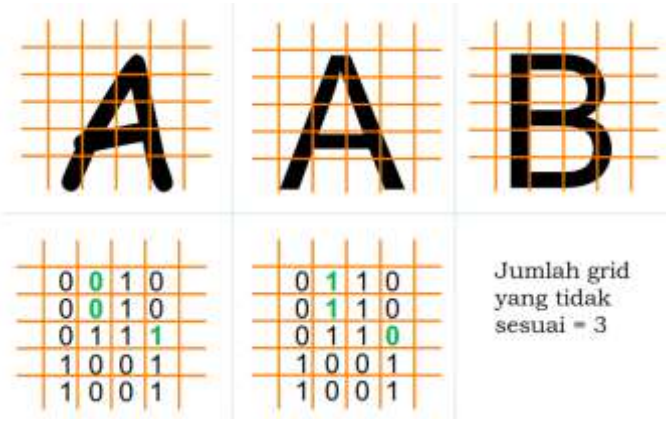
Regular expression untuk mengenali pola tanggal

1) Regex (template): (\d{1,2}) ([A-Z][a-z]+) (\d{4})
2) Dapat digunakan untuk mengenali penulisan tanggal seperti:
   - 1 Juni 2021
   - 20 Agustus 2021

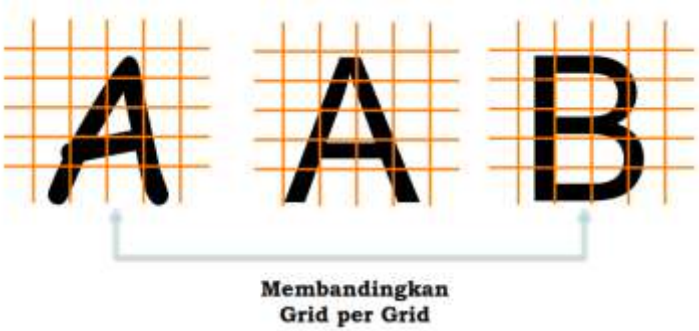
b. Pendekatan Statistik



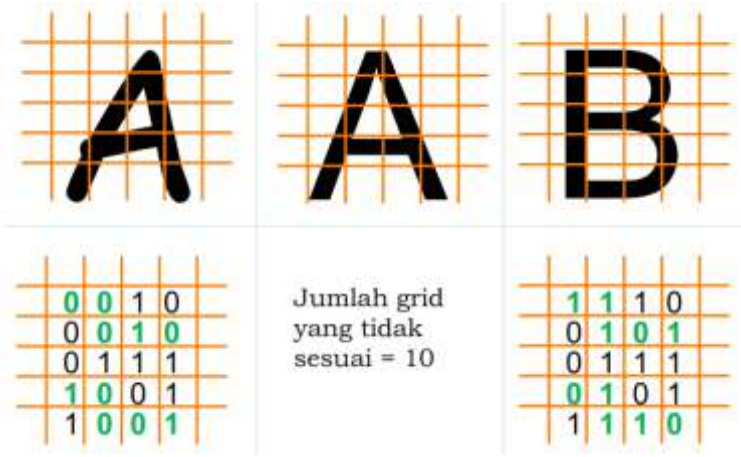
Gambar 3.9. Pola Huruf A dan B



Gambar 3.10. Hasil Identifikasi Pola Huruf A dan B



Gambar 3.11. Pola Huruf A dan B

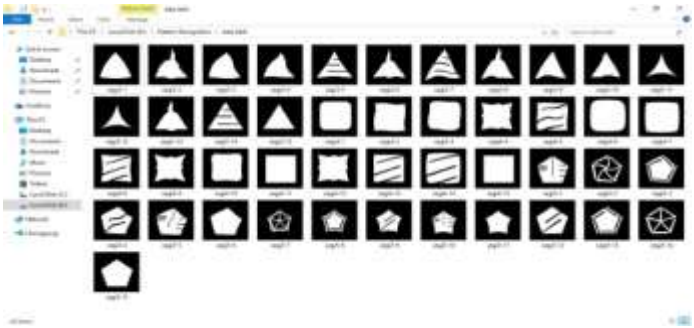


Gambar 3.12. Hasil Pola Huruf A dan B

4. *Train System*

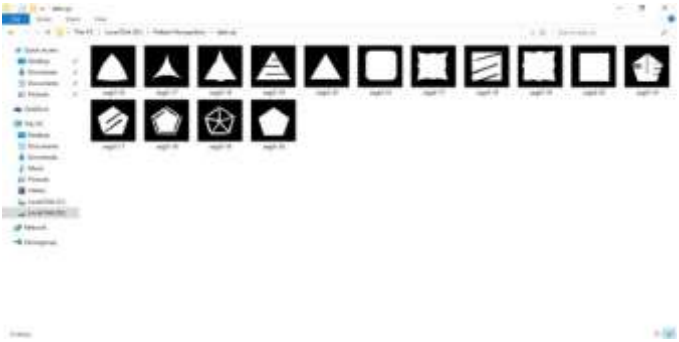
Berikut ini merupakan contoh pemrograman matlab untuk mengklasifikasi bentuk suatu objek dalam citra digital menggunakan algoritma jaringan saraf tiruan propagasi balik (*backpropagation neural network*). Pada contoh ini dilakukan pengklasifikasian terhadap bentuk segi-3, segi-4, dan segi-5. Ciri yang digunakan untuk membedakan ketiga jenis bentuk tersebut adalah *metric* dan *eccentricity. Metric* merupakan nilai perbandingan antara luas dan keliling objek. Sedangkan *eccentricity* merupakan nilai perbandingan antara jarak *foci ellips minor* dengan *foci ellips mayor* suatu objek. (Materi mengenai ekstraksi ciri lebih lanjut dapat dilihat pada laman berikut ini: Ekstraksi Ciri Citra). Langkah-langkah pemrograman matlab untuk mengklasifikasi bentuk suatu objek dalam citra digital menggunakan matlab adalah sebagai berikut:

1. Menyiapkan data latih untuk proses pelatihan (*training*). Pada proses ini digunakan 45 citra data latih yang terdiri dari 15 citra segi-3, 15 citra segi-4, dan 15 citra segi-5.



Gambar 3.13. Citra input Pola

2. Menyiapkan data uji untuk proses pengujian *(testing)*. Pada proses ini digunakan 15 citra data uji yang terdiri dari 5 citra segi-3, 5 citra segi-4, dan 5 citra segi-5.



Gambar 3.14. Hasil Pengujian Citra Pola

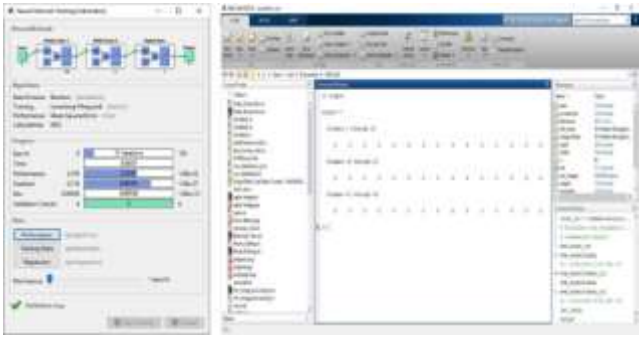
3. Mengekstrak ciri masing-masing bentuk berdasarkan parameter *eccentricity* dan *metric.*
   a. clc;clear;close all;
   b. image_folder = 'Pattern Recognition\data latih';

c. filenames = dir(fullfile(image_folder, '*.gif'));
d. total_images = numel(filenames);
e. **for** n = 1:total_images
f. full_name= fullfile(image_folder, filenames(n).name);
g. our_images = logical(imread(full_name));
h. our_images = bwconvhull(our_images,'objects');
i. stats= regionprops (our_images,'Area','Perimeter', 'Eccentricity');
j. area(n) = stats.Area;
k. perimeter(n) = stats.Perimeter;
l. metric(n) = 4*pi*area(n)/(perimeter(n)^2);
m. eccentricity(n) = stats.Eccentricity;
n. input = [metric;eccentricity];
o. target = zeros(1,45);
p. target(:,1:15) = 3;
q. target(:,16:30) = 4;
r. target(:,31:45) = 5;
s. end

4. Nilai *metric* dan *eccentricity* yang telah diekstrak kemudian dijadikan sebagai data masukan pada jaringan saraf tiruan *backpropagation*. Sedangkan pada data target digunakan nilai 3 untuk kelas segi-3, nilai 4 untuk kelas segi-4, dan nilai 5 untuk kelas segi-5. Langkah selanjutnya yaitu membangun jaringan dengan arsitektur 2-10-5-1 yang artinya memiliki 2 data masukan yaitu *metric* dan *eccentricity*, memiliki 2 layer tersembunyi *(hidden layer)* di mana pada hidden layer pertama berisi 10 neuron dan pada hidden layer kedua berisi 5 neuron. Dan memiliki 1 data keluaran yaitu jenis bentuk (segi-3, segi-4, atau segi-5).

a. net = newff(input,target,[10
   5],{'logsig','logsig'},'trainlm');
b. net.trainParam.epochs = 100;
c. net.trainParam.goal = 1e-5;
d. net = train(net,input,target);
e. output = round(sim(net,input))
f. save net.mat net

5. Sehingga dihasilkan tampilan pelatihan jaringan seperti pada gambar berikut:



Gambar 3.15. Hasil Klasifikasi Citra Pola

6. Pembahasan terkait perbandingan antara nilai keluaran JST pada proses pelatihan dengan data target latih ditunjukkan pada tabel di berikut:

No.	Kelas Keluaran JST	Kelas Target
1	3	3
2	3	3
3	3	3
4	3	3
5	3	3
6	3	3
7	3	3
8	3	3
9	3	3
10	3	3
11	3	3
12	3	3
13	3	3
14	3	3
15	3	3
16	4	4
17	4	4
18	4	4
19	4	4
20	4	4
21	5	4
22	4	4
23	4	4
24	4	4
25	4	4
26	4	4
27	4	4
28	5	4
29	4	4
30	4	4
31	5	5
32	5	5
33	5	5
34	5	5
35	5	5
36	5	5
37	5	5
38	5	5
39	5	5
40	5	5
41	5	5
42	5	5
43	5	5
44	5	5
45	5	5

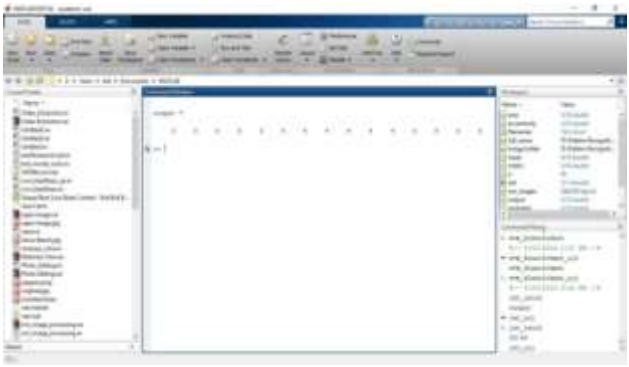
Gambar 3.16. Hasil Klasifikasi Pola

Pada tabel di atas, terdapat dua data yang diklasifikasikan secara salah (tidak sesuai dengan target) yaitu data ke-21 dan data ke-28. Sehingga akurasi yang dihasilkan JST pada proses pelatihan adalah (43/45) x 100% = 95,56%. Nilai akurasi tersebut menunjukkan bahwa JST cukup baik dalam mengklasifikasikan pola bentuk objek dari citra yang diberikan.

7. Sedangkan pemrograman untuk proses pengujian adalah:
   a. clc;clear;close all;
   b. image_folder = 'Pattern Recognition\data uji';
   c. filenames = dir(fullfile(image_folder, '*.gif'));
   d. total_images = numel(filenames);
   e. **for** n = 1:total_images
   f. full_name= fullfile(image_folder, filenames(n).name);
   g. our_images = logical(imread(full_name));
   h. our_images = bwconvhull(our_images,'objects');
   i. stats = regionprops(our_images,'Area','Perimeter','Eccentricity');
   j. area(n) = stats.Area;

k. perimeter(n) = stats.Perimeter;
l. metric(n) = (4*pi*area(n))./(perimeter(n).^2);
m. eccentricity(n) = stats.Eccentricity;
n. input = [metric;eccentricity];
o. **end**
p. load net
q. output = round(sim(net,input))

8. Nilai keluaran yang dihasilkan pada proses pengujian adalah:



Gambar 3.17. Hasil Pengujian Klasifikasi Pola

Perbandingan antara nilai kelaran JST pada proses pengujian dengan data target ditunjukkan pada tabel di bawah ini :

No	Kelas Keluaran JST	Kelas Target
1	3	3
2	3	3
3	3	3
4	3	3
5	3	3
6	4	4
7	4	4
8	4	4
9	4	4
10	4	4
11	4	5
12	5	5
13	5	5
14	5	5
15	5	5

Gambar 3.18. Hasil Klasifikasi Kelas yang dihasilkan

Berdasarkan data pada tabel tersebut terdapat satu data yang diklasifikasikan ke dalam kelas yang salah (tidak sesuai dengan target) yaitu data ke-11. Sehingga akurasi yang dihasilkan JST dalam proses pengujian adalah (14/15) x 100% = 93,33%. Dengan demikian, dapat dikatakan bahwa JST dapat mengklasifikasikan pola bentuk objek dalam citra dengan baik.

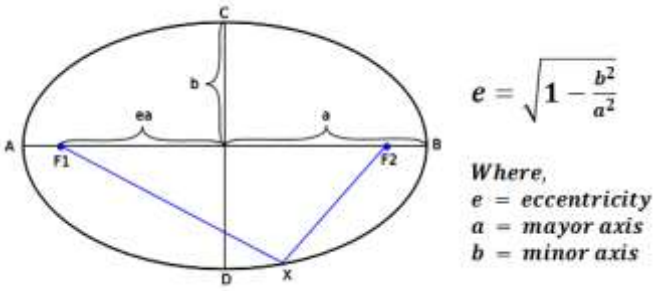
Berdasarkan data pada tabel tersebut terdapat satu data yang diklasifikasikan ke dalam kelas yang salah (tidak sesuai dengan target) yaitu data ke-11. Sehingga akurasi yang dihasilkan JST dalam proses pengujian adalah (14/15) x 100% = 93,33%. Dengan demikian, dapat dikatakan bahwa JST dapat mengklasifikasikan pola bentuk objek dalam citra dengan baik. Materi mengenai jaringan saraf tiruan untuk mengidentifikasi wajah.

Ekstraksi ciri citra merupakan tahapan mengekstrak ciri/informasi dari objek di dalam citra yang ingin dikenali/dibedakan dengan objek lainnya. Ciri yang telah diekstrak kemudian digunakan sebagai parameter/nilai masukan untuk membedakan antara objek satu dengan lainnya pada

tahapan identifikasi/ klasifikasi. Ciri yang umumnya diekstrak antara lain:

1. *Ekstraksi Ciri Bentuk*

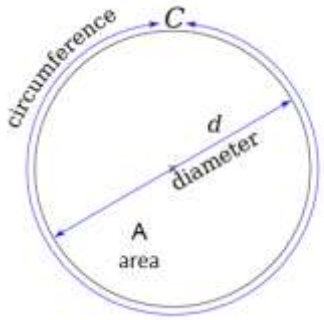
   Untuk membedakan bentuk objek satu dengan objek lainnya, dapat menggunakan parameter yang disebut dengan '*eccentricity*'**.** *Eccentricity* merupakan nilai perbandingan antara jarak *foci ellips minor* dengan *foci ellips mayor* suatu objek. *Eccentricity* memiliki rentang nilai antara 0 hingga 1. Objek yang berbentuk memanjang/ mendekati bentuk garis lurus, nilai *eccentricity*-nya mendekati angka 1, sedangkan objek yang berbentuk bulat/lingkaran, nilai *eccentricity*-nya mendekati angka 0. Penghitungan *eccentricity* diilustrasikan pada gambar di bawah ini:



Gambar 3.19. Perhitungan *Eccentricity*

Parameter lainnya yang dapat digunakan untuk membedakan bentuk suatu objek yaitu *'metric'*. *Metric* merupakan nilai perbandingan antara luas dan keliling objek. *Metric* memiliki rentang nilai antara 0 hingga 1. Objek yang berbentuk memanjang/mendekati bentuk garis lurus, nilai metricnya mendekati angka 0, sedangkan objek

yang berbentuk bulat/lingkaran, nilai *metric*-nya mendekati angka 1. Penghitungan metric diilustrasikan pada gambar di bawah ini:



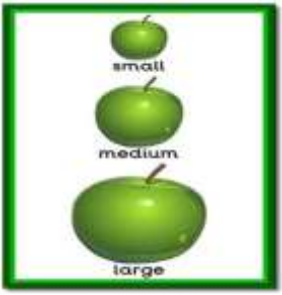
$$M = \frac{4\pi \times A}{C^2}$$

Where,
M = Metric
A = Area
C = Circumference

Gambar 3.20. Penghitungan *Metric*

2. *Ekstraksi Ciri Ukuran*

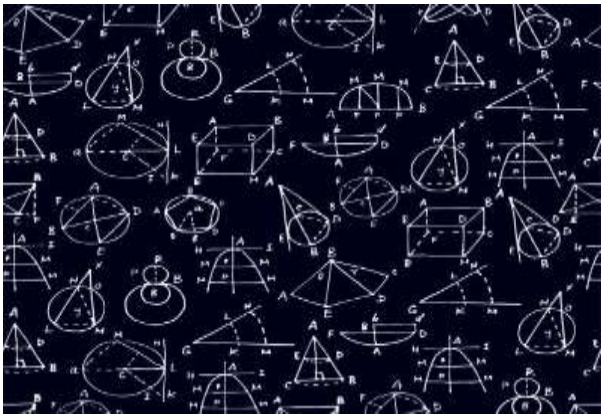
   Untuk membedakan ukuran objek satu dengan objek lainnya dapat menggunakan parameter luas dan keliling. Luas merupakan banyaknya piksel yang menyusun suatu objek. Sedangkan keliling merupakan banyaknya piksel yang mengelilingi suatu objek. Materi mengenai pemrograman matlab untuk menghitung luas dan keliling suatu objek dapat dilihat pada laman berikut ini: Cara menghitung luas dan keliling suatu citra



Gambar 3.21. Penghitungan Luas Area

3. *Ekstraksi Ciri Geometri*

Ciri geometri merupakan ciri yang didasarkan pada hubungan antara dua buah titik, garis, atau bidang dalam citra digital. Ciri geometri di antaranya adalah jarak dan sudut. Jarak antara dua buah titik (dengan satuan piksel) dapat ditentukan menggunakan persamaan euclidean, minkowski, manhattan, dll. Jarak dengan satuan piksel tersebut dapat dikonversi menjadi satuan panjang seperti milimeter, centimeter, meter, dll dengan cara membaginya dengan resolusi spasial (materi mengenai perhitungan jarak dapat dilihat pada laman berikut ini: Cara mengukur jarak antara dua objek dalam citra). Sedangkan sudut antara dua buah garis dapat ditentukan dengan perhitungan trigonometri maupun dengan analisis vektor.



Gambar 3.22. Perhitungan Trigonometri

4. *Ekstraksi Ciri Tekstur*

Untuk membedakan tekstur objek satu dengan objek lainnya dapat menggunakan ciri statistik orde pertama atau ciri statistik orde dua. Ciri orde pertama didasarkan pada karakteristik histogram citra. Ciri orde pertama

umumnya digunakan untuk membedakan tekstur makro-struktur (perulangan pola lokal secara periodik). Ciri orde pertama antara lain: *mean, variance, skewness, kurtosis*, dan *entropy*. Sedangkan ciri orde dua didasarkan pada probabilitas hubungan ketetanggaan antara dua piksel pada jarak dan orientasi sudut tertentu. Ciri orde dua umumnya digunakan untuk membedakan tekstur mikro-struktur (pola lokal dan perulangan tidak begitu jelas). Ciri orde dua antara lain: *Angular Second Moment, Contrast, Correlation, Variance, Inverse Different Moment,* dan *Entropy.*

Analisis tekstur juga dapat dilakukan dalam domain frekuensi antara lain menggunakan filter bank Gabor.

Gambar 3.23. Perhitungan Filter Bank Gabor

5. *Ekstraksi Ciri Warna*

   Untuk membedakan suatu objek dengan warna tertentu dapat menggunakan nilai hue yang merupakan represen-tasi dari cahaya tampak (merah, jingga, kuning, hijau, biru, ungu). Nilai hue dapat dikombinasikan dengan nilai *saturation* dan *value* yang merupakan tingkat kecerahan suatu warna. Untuk mendapatkan ketiga nilai tersebut, perlu dilakukan konversi ruang warna citra yang semula

RGB (Red, Green, Blue) menjadi HSV (Hue, Saturation, Value) melalui persamaan berikut:

R‘ = R/255

G‘ = G/255

B‘ = B/255

Cmax = max(R‘, G‘, B‘)

Cmin = min(R‘, G‘, B‘)

Δ = Cmax – Cmin

Perhitungan nilai Hue:

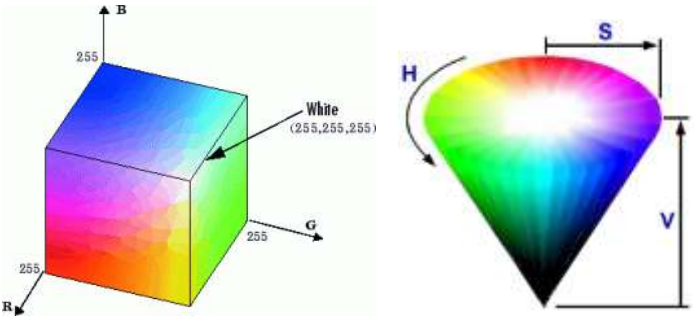
$$H = \begin{cases} 0^\circ & \Delta = 0 \\ 60^\circ \times \left(\frac{G'-B'}{\Delta} mod 6\right) & , C_{max} = R' \\ 60^\circ \times \left(\frac{B'-R'}{\Delta} + 2\right) & , C_{max} = G' \\ 60^\circ \times \left(\frac{R'-G'}{\Delta} + 4\right) & , C_{max} = B' \end{cases}$$

Perhitungan nilai Saturation:

$$S = \begin{cases} 0 & , C_{max} = 0 \\ \frac{\Delta}{C_{max}} & , C_{max} \neq 0 \end{cases}$$

Perhitungan nilai Value:

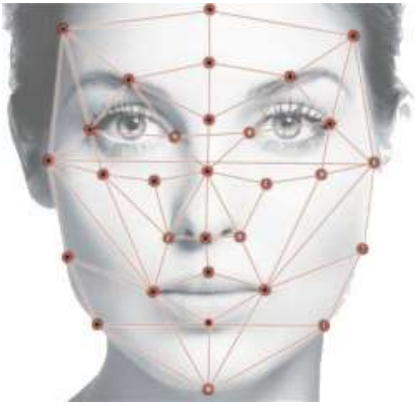
V = Cmax, sehingga ruang warna citra yang semula berbentuk kubus berubah bentuk menjadi kerucut.



Gambar 3.24. Jaringan Saraf Tiruan untuk Identifikasi Wajah

Berikut ini merupakan contoh pemrograman jaringan saraf tiruan *backpropagation* sederhana untuk identifikasi wajah seseorang berdasarkan ciri mata, hidung, mulut, dan telinga.

a. Langkah pertama yaitu mempersiapkan data untuk proses pelatihan dan pengujian Berikut ini merupakan contoh data untuk proses pelatihan :



Gambar 3.25. Teknik Identifikasi Wajah

Tabel 3.3. Perhitungan Nilai Ciri dan Target

No	Ciri/ Feature				Target
	Mata	Hidung	Mulut	Telinga	Nama Orang
1	0.35	0.47	0.88	0.34	Adi
2	0.59	0.11	0.90	0.56	Budi
3	0.19	0.89	0.54	0.38	Candra
4	0.36	0.90	0.39	0.82	Dedi
5	0.58	0.45	0.80	0.91	Erik
6	0.40	0.45	0.80	0.35	Adi
7	0.61	0.11	0.90	0.55	Budi
8	0.20	0.87	0.56	0.41	Candra
9	0.38	0.88	0.35	0.85	Dedi
10	0.57	0.46	0.82	0.92	Erik
11	0.33	0.45	0.85	0.37	Adi
12	0.55	0.14	0.90	0.57	Budi
13	0.18	0.87	0.55	0.40	Candra
14	0.38	0.89	0.37	0.85	Dedi
15	0.56	0.47	0.83	0.91	Erik

Sedangkan contoh data untuk pengujian adalah sebagai berikut:

Tabel 3.4. Perhitungan Nilai Data Ciri dan Target

No	Ciri/ Feature				Target
	Mata	Hidung	Mulut	Telinga	Nama Orang
1	0.38	0.43	0.85	0.34	Adi
2	0.60	0.14	0.87	0.57	Budi
3	0.19	0.88	0.60	0.40	Candra
4	0.35	0.90	0.41	0.83	Dedi
5	0.59	0.45	0.78	0.93	Erik

b. Langkah berikutnya yaitu menyusun data latih beserta target latih sesuai dengan format pemrograman JST di Matlab. Data latih disusun sehingga menjadi matriks berukuran 4 x 15 seperti berikut ini : Sedangkan target latih disusun menjadi matriks berukuran 1 x 15 seperti berikut ini :

Tabel 3.5. Hasil Perhitungan Ciri dan Target

1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
0.35	0.59	0.19	0.36	0.58	0.40	0.61	0.20	0.38	0.57	0.33	0.55	0.18	0.38	0.56
0.47	0.11	0.89	0.90	0.45	0.45	0.11	0.87	0.88	0.46	0.45	0.14	0.87	0.89	0.47
0.88	0.90	0.54	0.39	0.80	0.80	0.90	0.56	0.35	0.82	0.85	0.90	0.55	0.37	0.83
0.34	0.56	0.38	0.82	0.91	0.35	0.55	0.41	0.85	0.92	0.37	0.57	0.40	0.85	0.91

Keterangan: 1 = Adi, 2 = Budi, 3 = Candra, 4 = Dedi, 5 = Erik

c. Langkah selanjutnya yaitu menuliskan coding pada script matlab seperti berikut ini: Coding 3.1. untuk menuliskan data latih dan target latih pada matlab adalah sebagai berikut :

```
% Mempersiapkan data latih dan target latih
data_latih = [0.35,0.59,0.19,0.36,0.58,0.40,0.61,0.20,
0.38,0.57,0.33,0.55,0.18,0.38,0.56;...
0.47,0.11,0.89,0.90,0.45,0.45,0.11,0.87,0.88,0.46,0.45,0.
14,0.87,0.89,0.47;...
0.88,0.90,0.54,0.39,0.80,0.80,0.90,0.56,0.35,0.82,0.85,0.
90,0.55,0.37,0.83;...
0.34,0.56,0.38,0.82,0.91,0.35,0.55,0.41,0.85,0.92,0.37,0.
57,0.40,0.85,0.91];
target_latih = [1,2,3,4,5,1,2,3,4,5,1,2,3,4,5];
[~, N] = size (data_latih);
```

Coding 3.2. Selanjutnya membuat coding Jaringan Saraf Tiruan *Backpropagation* dengan arsitektur 4-2-1 dan inisialisasi bobot awal secara acak. Pada pemrograman ini digunakan fungsi aktivasi sigmoid biner (logsig) pada *hidden layer* dan fungsi aktivasi linear (purelin) pada layer keluaran. Sedangkan fungsi pelatihan menggunakan metode *gradien descent*

```
% Pembuatan JST
Net = newff(minmax(data_latih),[2 1],{'logsig','purelin'},
'traingdx');
net.IW {1, 1} = [-7.62, 0.97,-2.60,-9.55;-5.83,-3.41, 3.08,-
4.44];
net.LW {2, 1} = [-2.40,-2.67];
net.b {1, 1} = [9.38;-2.7];
net.b {2, 1} = 5.93;
```

Coding 3.3. Membuat coding untuk memberikan parameter-parameter yang mempengaruhi proses

pelatihan jst seperti parameter jumlah epoch, target error, learning rate, momentum.

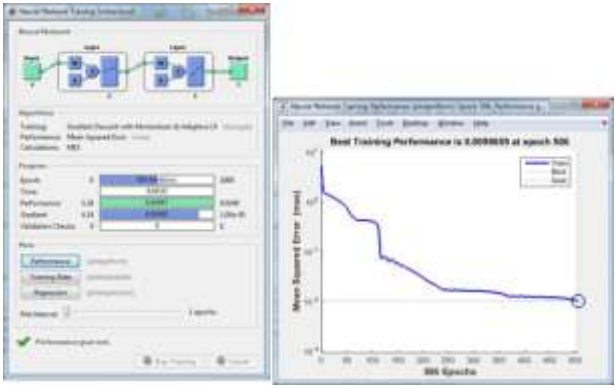
% Memberikan nilai untuk mempengaruhi proses pelatihan

1. net.performFcn = 'mse';
2. net.trainParam.goal = 0.01;
3. net.trainParam.show = 20;
4. net.trainParam.epochs = 1000;
5. net.trainParam.mc = 0.95;
6. net.trainParam.lr = 0.1;

Coding 3.4 Membuat coding untuk melakukan pelatihan jaringan

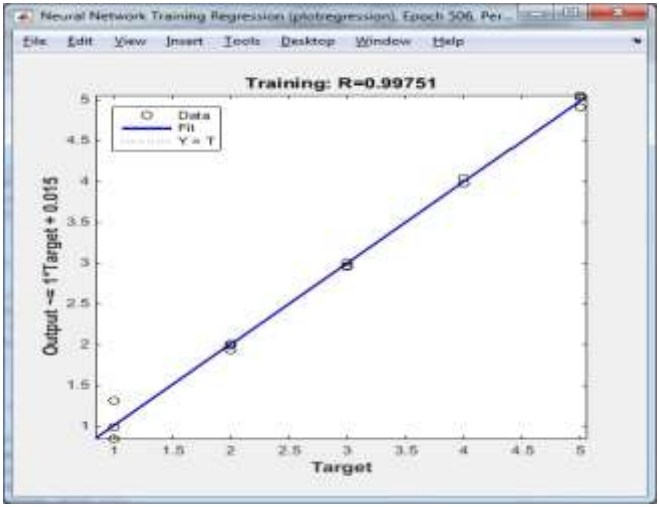
```
% Proses training
[net_keluaran,tr,Y,E] = train(net,data_latih,target_latih);
```

Sehingga muncul tampilan seperti berikut: Pada tampilan tersebut ditunjukkan bahwa target error (mse) tercapai pada epoch ke 506. Kita bisa melihat error (mse) yang dihasilkan pada setiap epoch dengan meng-klik tombol ‘performance’ sehingga muncul tampilan seperti berikut:



Gambar 3.26. Hasil Perhitungan Ciri dan Target epoch

Sedangkan koefisien korelasi hasil pelatihan dapat dilihat dengan meng-klik tombol 'regression' sehingga diperoleh:



Gambar 3.27. Hasil Training Ciri dan Target

Nilai koefisien korelasi sebesar 0.99751 menunjukkan bahwa akurasi hasil proses pelatihan sangat baik.

Coding 3.5 Untuk melihat nilai-nilai hasil pelatihan, kita dapat menuliskan coding sbb:

```
% Hasil setelah pelatihan
1. bobot_hidden = net_keluaran.IW{1,1};
2. bobot_keluaran = net_keluaran.LW{2,1};
3. bias_hidden = net_keluaran.b{1,1};
4. bias_keluaran = net_keluaran.b{2,1};
5. jumlah_iterasi = tr.num_epochs;
6. nilai_keluaran = Y;
7. nilai_error = E;
8. error_MSE = (1/N)*sum(nilai_error.^2);
```

d. Langkah terakhir yaitu proses pengujian jaringan.

5. *Evaluate System*

Bagaimana memvalidasi hasil dari pengujian setelah dilakukan data *training.* Afar dapat diketahui berapakah tingkat kepercayaan hasil keputusan.

4.1 Data uji disusun seperti ditunjukkan oleh matriks berikut :

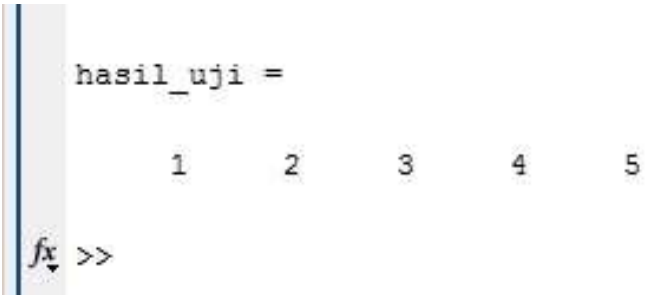
Tabel 3.6. Hasil Tingkat Kerpayaan

1	2	3	4	5
0.38	0.60	0.19	0.35	0.59
0.43	0.14	0.88	0.90	0.45
0.85	0.87	0.60	0.41	0.78
0.34	0.57	0.40	0.83	0.93

4.2 Dalam matlab kita dapat menuliskan coding sbb:

```
% Performa jaringan
data_uji = [0.38,0.60,0.19,0.35,0.59;...
            0.43,0.14,0.88,0.90,0.45;...
            0.85,0.87,0.60,0.41,0.78;...
            0.34,0.57,0.40,0.83,0.93];
hasil_uji = round(sim(net_keluaran,data_uji))
```

sehingga diperoleh hasil pada *command window* seperti berikut ini:



Gambar 3.28. Hasil Perhitungan Tingkat Kepercayaan

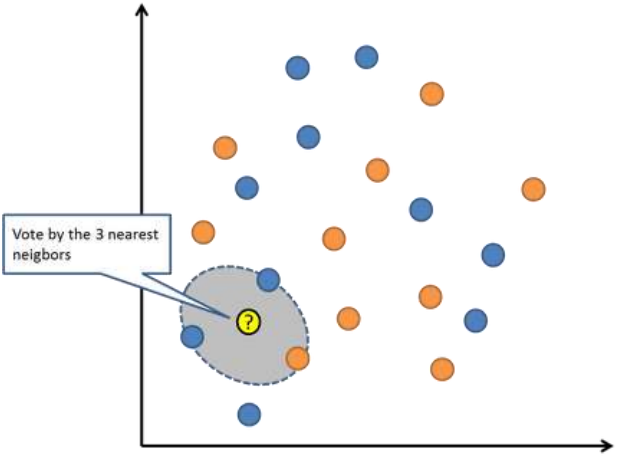
Hasil tersebut 100% sesuai dengan target uji yang telah diberikan sebelumnya. Pada contoh ini ditunjukkan bahwa JST dapat mengidentifikasi/membedakan pola wajah seseorang berdasarkan ciri mata, hidung, mulut, dan telinga dengan baik.

E. Teknik Klasifikasi dengan KNN

K-Nearest Neighbor (k-NN), "*Algoritma k-nearest neighbor (k-NN atau KNN) merupakan sebuah algoritma untuk melakukan*

klasifikasi terhadap objek berdasarkan data pembelajaran yang jaraknya paling dekat dengan objek tersebut."

Ilustrasi dari metode yang digunakan oleh algoritma k-nn ditunjukkan pada gambar di bawah ini:



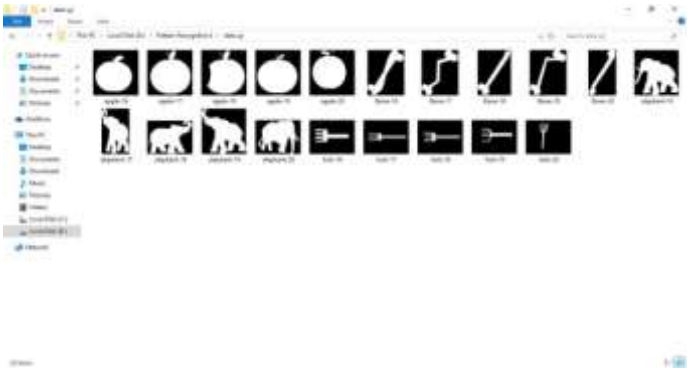
Gambar 3.29. Ilustrasi dari metode KNN

Berikut ini merupakan contoh aplikasi pemrograman matlab untuk mengklasifikasi citra digital berdasarkan pola bentuk menggunakan algoritma k-nearest neighbor. Pada contoh ini k-nn digunakan untuk mengklasifikasi bentuk dari citra apel, tulang, gajah, dan garpu. Ciri yang digunakan untuk membedakan keempat bentuk dari citra tersebut adalah *eccentricity* dan *metric*. Pemrograman matlab menggunakan algoritma k-nearest neighbor pada contoh ini dapat dijalankan minimal menggunakan matlab versi r2014a karena menggunakan fungsi baru yaitu fitcknn (*fit k-nearest neighbor classifier*). Langkah-langkah pemrograman matlab untuk mengklasifikasikan bentuk suatu objek dalam citra digital yaitu

1. Mempersiapkan citra untuk proses pelatihan. Pada proses tersebut digunakan 60 citra yang terdiri dari 15 citra apel, 15 citra tulang, 15 citra gajah, dan 15 citra garpu

Gambar 3.30. Citra Untuk Proses Pelatihan

2. Mempersiapkan citra untuk proses pengujian. Pada proses tersebut digunakan 20 citra yang terdiri dari 5 citra apel, 5 citra tulang, 5 citra gajah, dan 5 citra garpu



Gambar 3.31. Citra Hasil Proses Pelatihan

3. Setelah citra untuk proses pelatihan dan pengujian disiapkan, dilakukan pemrograman untuk kedua proses terse-

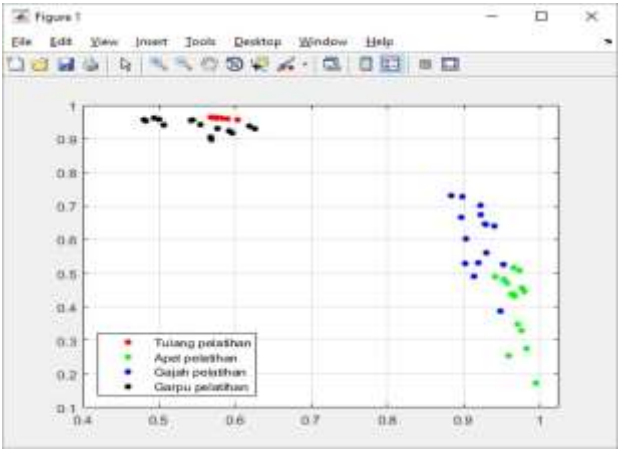
but. Source code untuk mengklasifikasi bentuk suatu objek dalam citra digital menggunakan algoritma k-nearest neighbor adalah sebagai berikut:

```
clc;clear;close all;

image_folder = 'data latih';
filenames = dir(fullfile(image_folder, '*.gif'));
total_images = numel(filenames);

for n = 1:total_images
full_name= fullfile(image_folder, filenames(n).name);
our_images = logical(imread(full_name));
our_images = bwconvhull(our_images,'objects');
stats = regionprops(our_images,'Area','Perimeter','Eccen
tricity');
area(n) = stats.Area;
perimeter(n) = stats.Perimeter;
metric(n) = 4*pi*area(n)/(perimeter(n).^2);
eccentricity(n) = stats.Eccentricity;
training = [metric;eccentricity]';

group = cell(60,1);
group(1:15,:) = {'tulang'};
group(16:30,:) = {'apel'};
group(31:45,:) = {'gajah'};
group(46:60,:) = {'garpu'};
end
figure,
gscatter(metric',eccentricity',group,'rgbk','.',15)
legend('Tulang pelatihan','Apel pelatihan','Gajah
pelatihan','Garpu pelatihan',...
```

```
'Location','SouthWest')
grid on

image_folder_uji = 'data uji';
filenames_uji = dir(fullfile(image_folder_uji, '*.gif'));
total_images_uji = numel(filenames_uji);
for n = 1:total_images_uji
full_name_uji = fullfile(image_folder_uji, filenames_uji(n).
name);
our_images_uji = logical(imread(full_name_uji));
our_images_uji = bwconvhull(our_images_uji,'objects');
stats_uji =
regionprops(our_images_uji,'Area','Perimeter','Eccentricity
');
area_uji(n) = stats_uji.Area;
perimeter_uji(n) = stats_uji.Perimeter;
metric_uji(n) = (4*pi*area_uji(n))./(perimeter_uji(n).^2);
eccentricity_uji(n) = stats_uji.Eccentricity;
sample = [metric_uji;eccentricity_uji]';
end
c = fitcknn(training, group,'NumNeighbors',1,'Standardize'
1);
Class = predict(c,sample);
figure,
gscatter(metric',eccentricity',group,'rgbk','.',15)
grid on
hold on
gscatter(metric_uji',eccentricity_uji',Class,[1 1 0; 1 0 1; 0 1
1; .5 .5 .5],'x',15);
legend('Tulang pelatihan','Apel pelatihan','Gajah
pelatihan','Garpu pelatihan',...
```

'Tulang pengujian','Garpu pengujian','Apel pengujian','Gajah pengujian',...
'Location','SouthWest')
hold off

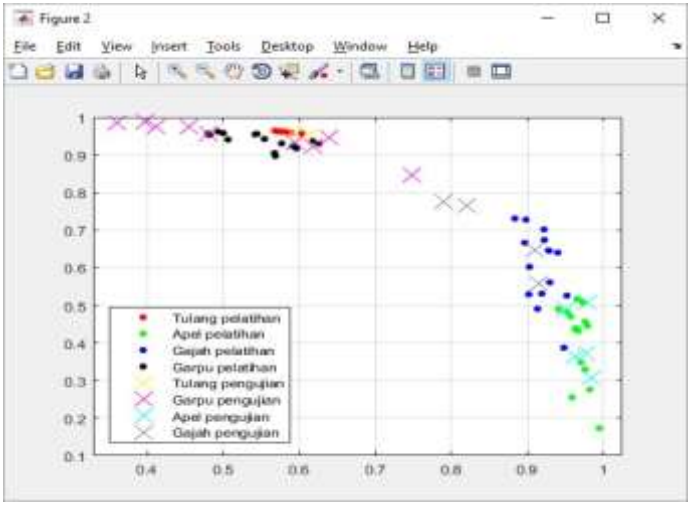
4. Sehingga pada proses pelatihan diperoleh hasil berupa grafik seperti pada gambar berikut.



Gambar 3.32. Citra Hasil Proses Klasifikasi KNN

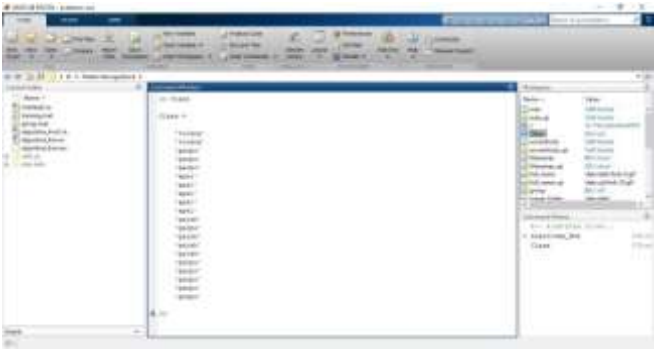
Pada grafik tersebut terlihat distribusi data (nilai metric dan *ecentricity*) pada masing-masing kelas grup (apel, tulang, gajah, garpu). Pada proses pengujian, suatu data uji dikatakan masuk ke dalam kelas grup apel apabila tetangga terdekat dari data uji tersebut dominan dengan kelas grup A.

5. Pada proses pengujian dihasilkan grafik seperti pada gambar di bawah ini.



Gambar 3.33. Hasil Proses Pengujian Klasifikasi KNN

6. Kelas keluaran yang dihasilkan dalam proses pengujian adalah sbb:



Gambar 3.34. Hasil Proses Klasifikasi KNN

Sehingga hasil perbandingan antara kelas keluaran dengan kelas target pada proses pengujian adalah:

Tabel 3.7. Perbandingan Antara Kelas Keluaran dengan kelas target

No	Kelas keluaran k-nn	Kelas Target
1	'tulang'	'tulang'
2	'tulang'	'tulang'
3	'garpu'	'tulang'
4	'garpu'	'tulang'
5	'garpu'	'tulang'
6	'apel'	'apel'
7	'apel'	'apel'
8	'apel'	'apel'
9	'apel'	'apel'
10	'apel'	'apel'
11	'gajah'	'gajah'
12	'garpu'	'gajah'
13	'gajah'	'gajah'
14	'gajah'	'gajah'
15	'gajah'	'gajah'
16	'garpu'	'garpu'
17	'garpu'	'garpu'
18	'garpu'	'garpu'
19	'garpu'	'garpu'
20	'garpu'	'garpu'

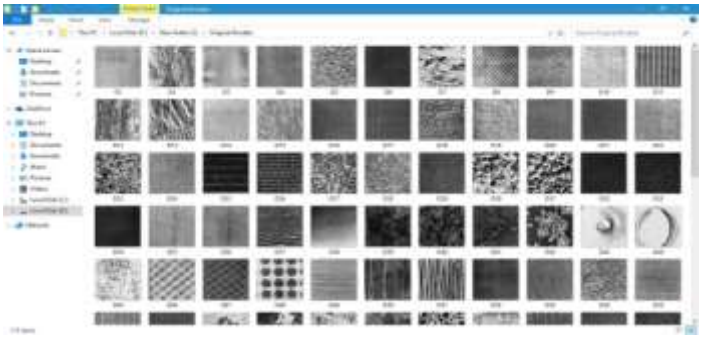
Berdasarkan tabel di atas, tampak bahwa terdapat empat buah data uji yang diklasifikasikan ke dalam kelas yang salah (tidak sesuai dengan kelas target). Sehingga akurasi sistem dalam mengklasifikasikan bentuk objek adalah (16/20) x 100% = 80%. Nilai akurasi tersebut menunjukkan bahwa algoritma k-nearest neighbor cukup baik dalam mengklasifikasikan bentuk objek pada citra yang diberikan.

F. Teknik Klasifikasi dengan Naive Bayes

K-means Clustering merupakan salah satu metode data clustering non hirarki yang berusaha mempartisi data yang ada ke dalam satu atau lebih cluster/kelompok. Metode ini mempartisi data ke dalam cluster/kelompok sehingga data yang memiliki karakteristik yang sama dikelompokkan ke dalam satu cluster yang sama dan data yang mempunyai

karakteristik yang berbeda dikelompokkan ke dalam kelompok yang lain. Sedangkan Naive Bayes Classifier merupakan salah satu metode *machine learning* yang memanfaatkan perhitungan probabilitas dan statistik. Metode ini dikemukakan oleh ilmuwan Inggris yaitu Thomas Bayes untuk memprediksi probabilitas di masa depan berdasarkan pengalaman di masa sebelumnya.

Berikut ini merupakan contoh aplikasi pemrograman matlab (menggunakan Matlab R2015b) mengenai pola tekstur citra menggunakan algoritma k means clustering dan naive bayes classifier. Citra yang digunakan adalah citra tekstur Brodatz sejumlah 112 buah seperti tampak pada gambar di bawah ini:



Gambar 3.35. Citra Input untuk Naive Bayes

Langkah pertama yang dilakukan adalah melakukan ekstraksi ciri tekstur citra menggunakan metode *Gray Level Co-Occurence Matrix* (GLCM). Metode ini pertama kali dikenalkan oleh Robert M Haralick (bersama dengan K. Shanmugam and I. Dinstein) dalam publikasi yang berjudul *"Textural Features for Image Classification"* pada IEEE Transactions on Systems, Man, and Cybernetics, Vol. SMC-3,

No. 6, November 1973, pp. 610-621. Prinsip dari metode ini yaitu menghitung probabilitas hubungan ketetanggaan antara dua piksel pada jarak dan orientasi sudut tertentu. Pendekatan ini bekerja dengan membentuk sebuah matriks kookurensi dari data citra, dilanjutkan dengan menentukan ciri sebagai fungsi dari matriks antara tersebut.

Kookurensi berarti kejadian bersama, yaitu jumlah kejadian satu level nilai piksel bertetangga dengan satu level nilai piksel lain dalam jarak (d) dan orientasi sudut (θ) tertentu. Jarak dinyatakan dalam piksel dan orientasi dinyatakan dalam derajat. Orientasi dibentuk dalam empat arah sudut dengan interval sudut 45º , yaitu 0º, 45º, 90º, dan 135º. Sedangkan jarak antar piksel dapat ditetapkan sebesar 1 piksel, 2 piksel, atau lebih. Matriks kookurensi merupakan matriks bujursangkar dengan jumlah elemen sebanyak kuadrat jumlah level intensitas piksel pada citra. Setiap titik (p,q) pada matriks kookurensi berorientasi berisi peluang kejadian piksel bernilai p bertetangga dengan piksel bernilai q pada jarak d serta orientasi θ dan (180º-θ).

Parameter tekstur yang dapat diekstrak dengan metode GLCM adalah *angular second moment, contrast, correlation, variance, inverse difference moment, sum average, sum variance, sum entropy, entropy, difference variance, difference entropy,* dan information *measures of correlation.*

Namun pada contoh ini, hanya menggunakan dua parameter yaitu *contrast* dan *correlation.*

Kedua parameter tersebut dijadikan sebagai nilai masukan dalam algoritma k means dan naive bayes. Algoritma k means digunakan untuk mengkluster 112 citra tekstur brodatz menjadi tiga kelompok.

Sedangkan algoritma naive bayes digunakan untuk mengklasifikasikan citra dengan target berupa kelas keluaran

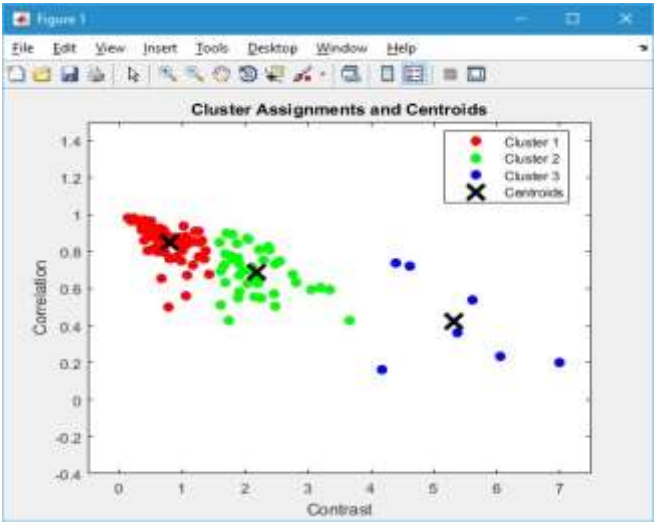
dari algoritma k means. Hasil keluaran algoritma naive bayes kemudian dibandingkan dengan hasil keluaran pada algoritma k means sehingga diperoleh nilai akurasi.

Koding untuk membaca citra, melakukan ekstraksi ciri tekstur, dan clustering adalah sebagai berikut:

```
1.  clc;clear;close all;
2.  image_folder = 'Original Brodatz';
3.  filenames = dir(fullfile(image_folder, '*.gif'));
4.  total_images = numel(filenames);
5.  for n = 1:total_images
6.  full_name = fullfile(image_folder, filenames(n).name);
7.  Img = imread(full_name);
8.  GLCM = graycomatrix(Img,'Offset',[0 1; -1 1; -1 0; -1 -1]);
9.  stats = graycoprops(GLCM,{'contrast','correlation','energy',
    'homogeneity'});
10. CON(n) = mean(stats.Contrast);
11. CORR(n) = mean(stats.Correlation);
12. X = [CON;CORR]';
13. end
14. opts = statset('Display','final');
15. [idx,C] = kmeans(X,3,'Distance','sqeuclidean',...
16. 'Replicates',5,'Options',opts);
17. figure;
18. plot(X(idx==2,1),X(idx==2,2),'r.','MarkerSize',24)
19. hold on
20. plot(X(idx==1,1),X(idx==1,2),'g.','MarkerSize',24)
21. plot(X(idx==3,1),X(idx==3,2),'b.','MarkerSize',24)
22. plot(C(:,1),C(:,2),'kx',...
23. 'MarkerSize',15,'LineWidth',3)
24. legend('Cluster 1','Cluster 2','Cluster 3','Centroids',...
25. 'Location','best')
26. title('Cluster Assignments and Centroids')
```

```
27. xlabel('Contrast')
28. ylabel('Correlation')
29. h = gca;
30. xlim(h.XLim+.5*[-1,1])
31. ylim(h.YLim+.5*[-1,1])
32. hold off
```

sehingga diperoleh grafik keluaran seperti pada gambar berikut:



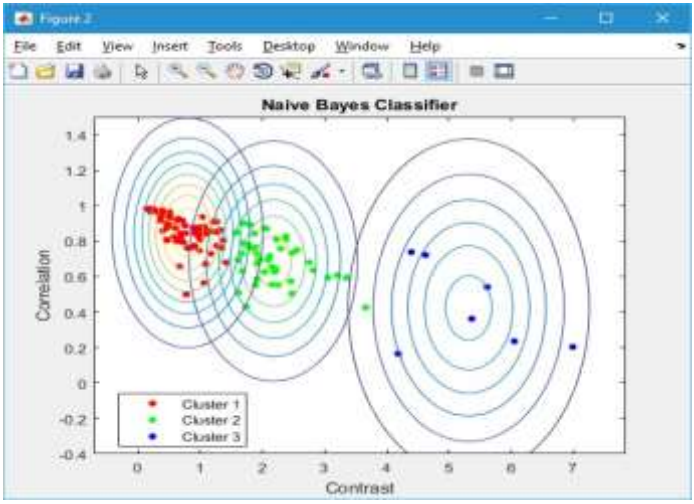
Gambar 3.36. Hasil Klasifikasi dengan Naive Bayes

Grafik di atas menunjukkan bahwa algoritma k means telah mengelompokkan 112 citra tekstur brodatz menjadi tiga kelompok (Cluster 1, Cluster 2, dan Cluster 3). Kemudian kelompok pada masing-masing citra tersebut dijadikan sebagai target keluaran pada algoritma naive bayes untuk melakukan klasifikasi. Koding untuk melakukan klasifikasi menggunakan algoritma naive bayes adalah:

```
Y = cell(numel(idx),1);
for n = 1:numel(Y)
if idx(n,:) == 1
Y{n,:} = 'Cluster 1';
elseif idx(n,:) == 2
Y{n,:} = 'Cluster 2';
else
Y{n,:} = 'Cluster 3';
end
end
Mdl = fitcnb(X,Y);
figure
gscatter(X(:,1),X(:,2),Y);
h = gca;
xylim = [h.XLim h.YLim]; % Get current axis limits
hold on
Params = cell2mat(Mdl.DistributionParameters);
Mu = Params(2*(1:3)-1,1:2); % Extract the means
Sigma = zeros(2,2,3);
for j = 1:3
Sigma(:,:,j) = diag(Params(2*j,:)); % Extract the standard deviations
ezcontour(@(x1,x2)mvnpdf([x1,x2],Mu(j,:),Sigma(:,:,j)),...
xylim+0.5*[-1,1,-1,1]) ...
% Draw contours for the multivariate normal distributions
end
title('Naive Bayes Classifier')
xlabel('Contrast')
ylabel('Correlation')
legend('Cluster 1','Cluster 2','Cluster 3',...
'Location','best')
hold off
```

```
32. isLabels = resubPredict(Mdl);
33. accuracy = sum(strcmp(isLabels,Y))/numel(Y)*100
```

Sehingga diperoleh grafik keluaran seperti pada gambar di bawah ini:



Gambar 3.37. Hasil Pengujian dengan Naive Bayes

Grafik tersebut menunjukkan bahwa algoritma naive bayes telah mengklasifikasikan citra tekstur pada masing-masing kelompok/kelas. Sebagai validasi, kelas keluaran dari algoritma naive bayes kemudian dibandingkan dengan kelas keluaran dari algoritma k means. Pada kelas keluaran algoritma naive bayes terdapat 108 citra yang memiliki kelas yang sama dengan kelas keluaran dari algoritma k means sehingga diperoeh akurasi sebesar 108/112*100 = 96.4286%. Nilai akurasi tersebut menunjukkan bahwa algoritma naive bayes mampu mengklasifikasi citra tekstur dengan sangat baik.

04 Penerapan Teknologi Biometrik

A. Biometrik Sidik Jari

Sidik jari manusia ini merupakan bukti materi yang amat penting. Akurasi dalam melakukan identifikasi bergantung pada reliabilitas ciri yang diambil dari citra sidik jari. Pada penelitian ini untuk menghasilkan ciri-ciri sidik jari digunakan metode pendekatan karakteristik fraktal. Pendekatan fraktal dipilih didasari pada pertimbangan bahwa struktur garis-garis sidik jari bersifat alami dan tidak teratur, dan fraktal dikenal sebagai metode yang sangat cocok untuk keadaan alami dan tidak teratur tersebut. Adapun tahapan dalam mengolah data sidik jari pada penelitian ini adalah akuisisi citra, preprocessing, ekstraksi ciri, dan pencocokan.

Akuisisi citra adalah tahap yang diawali dengan menangkap/mengambil gambar sidik jari dengan menggunakan scanner. Citra sidik jari yang diolah adalah citra grayscale dengan 256 tingkat keabuan dan memiliki dimensi 320 x 320 pixel, dengan kerapatan gambar 300 dpi. Tahapan *preprocessing* meliputi beberapa tahapan yaitu normalisasi orientasi, segmentasi, perbaikan citra (*enhancement*), ekstraksi bukit dan penipisan. Ekstraksi ciri merupakan proses untuk menghasilkan ciri sidik jari, yaitu dengan menggunakan metode fraktal (kode fraktal, dimensi fraktal dan derajat kekosongan). Pencocokan adalah proses untuk identifikasi sidik jari. Sistem pengolahan citra sidik jari yang telah dibuat

untuk mendapatkan ekstraksi ciri ini telah dapat menentukan hasil identifikasi sidik jari dengan menghasilkan tiga ciri fraktal yaitu kode fraktal, dimensi fraktal dan derajat kekosongan.

B. Biometrik Wajah

Sistem pengenalan wajah adalah teknologi yang mampu mengidentifikasi atau memverifikasi seseorang dari gambar digital atau bingkai video dari sumber video. Sistem pengenalan wajah bekerja dengan beberapa metode, tetapi secara umum, sistem ini bekerja dengan membandingkan fitur wajah yang dipilih dari gambar yang diberikan dengan wajah dalam database. Sistem Ini juga digambarkan sebagai aplikasi berbasis kecerdasan buatan biometrik (*biometric artificial intelligence*) yang dapat secara unik mengidentifikasi seseorang dengan menganalisis pola berdasarkan tekstur dan bentuk wajah orang tersebut.

Meskipun pada awalnya berbentuk aplikasi komputer, namun belakangan ini penggunaannya berkembang lebih luas lagi pada *platform mobile* dan dalam bentuk teknologi lainnya, seperti robot. Sistem ini biasanya digunakan sebagai akses kontrol dalam sistem keamanan dan dapat dibandingkan dengan biometrik lain seperti sistem pengenalan sidik jari atau iris mata. Meskipun sebagai teknologi biometrik keakuratan sistem pengenalan wajah lebih rendah daripada pengenalan iris dan pengenalan sidik jari, sistem ini diadopsi secara luas karena prosesnya yang tanpa kontak dan non-invasif. Baru-baru ini, sistem ini juga menjadi populer sebagai alat identifikasi dan pemasaran komersial. Penggunaan lainnya termasuk interaksi manusia-komputer tingkat lanjut, kamera pengawas, pengindeksan gambar secara otomatis, dan basis data video.

1. **Pengenalan Wajah 3-D (*3-Dimensional Recognition*)**

   Teknik pengenalan wajah tiga dimensi menggunakan sensor 3D untuk menangkap informasi bentuk wajah. Informasi ini kemudian digunakan untuk mengidentifikasi fitur-fitur khas pada permukaan wajah, seperti kontur rongga mata, hidung, dan dagu.

   Salah satu keuntungan dari pengenalan wajah 3D adalah tidak terpengaruh oleh perubahan pencahayaan seperti teknik lainnya. Teknik ini juga dapat mengidentifikasi wajah dari berbagai sudut pandang, termasuk tampilan profil. Poin data tiga dimensi dari wajah sangat meningkatkan ketepatan pengenalan wajah. Penelitian 3D ditingkatkan dengan pengembangan sensor canggih yang melakukan pekerjaan yang lebih baik dalam menangkap citra wajah 3D. Sensor bekerja dengan memproyeksikan cahaya terstruktur ke wajah. Hingga selusin atau lebih sensor gambar ini dapat ditempatkan pada chip CMOS yang sama—masing-masing sensor menangkap bagian berbeda dari sepktrum.

   Bahkan teknik pencocokan 3D yang sempurna bisa peka terhadap ekspresi wajah. Untuk tujuan itu, kelompok di Technion menerapkan alat dari geometri metrik untuk memperlakukan ekspresi wajah sebagai isometri.

   Metode terbaru adalah memperkenalkan cara untuk menangkap gambar 3D dengan menggunakan tiga kamera pelacak yang mengarah pada sudut yang berbeda; satu kamera akan mengarah ke depan subjek, yang kedua ke samping, dan yang ketiga pada sudut tertentu. Semua kamera ini akan bekerja bersama sehingga dapat melacak wajah subjek secara *real time* dan dapat mendeteksi dan mengenali wajah.

2. **Analisi Tekstur Kulit (*Skin Texture Analysis*)**
   Tren lain yang muncul menggunakan detail visual kulit, seperti yang ditangkap dalam gambar digital standar atau gambar yang dipindai. Teknik ini, yang disebut *Skin Texture Analysis*, mengubah garis, pola, dan bintik-bintik unik pada kulit seseorang menjadi ruang matematika. Analisis Tekstur Permukaan ini mampu mengidentifikasi perbedaan antara pasangan kembar identik, yang belum mungkin dilakukan hanya menggunakan perangkat lunak pengenalan wajah saja. Tes telah menunjukkan bahwa dengan penambahan analisis tekstur kulit, kinerja dalam mengenali wajah dapat meningkat 20 hingga 25 persen.

3. **Pengenalan Wajah Gabungan Berbagai Teknik (*Facial Recognition Combining Different Techniques*)**
   Karena setiap metode memiliki kelebihan dan kekurangan, perusahaan teknologi telah menggabungkan metode tradisional, Pengenalan 3-D dan Analisis Tekstual Kulit, untuk menciptakan sistem pengenalan wajah yang memiliki tingkat keberhasilan yang lebih tinggi. Teknik gabungan memiliki keunggulan dibandingkan sistem lain. Relatif tidak sensitif terhadap perubahan ekspresi, termasuk berkedip, mengerutkan kening atau tersenyum, dan memiliki kemampuan untuk mengimbangi pertumbuhan kumis atau janggut dan penampilan kacamata.

4. **Kamera Termal (*Thermal Cameras*)**
   Bentuk lain dari input data untuk pengenalan wajah adalah dengan menggunakan kamera termal, dengan prosedur ini kamera hanya akan mendeteksi bentuk kepala dan akan mengabaikan aksesori subjek seperti kacamata, topi, atau *makeup*. Tidak seperti kamera konvensional, kamera

termal dapat menangkap citra wajah bahkan dalam kondisi cahaya rendah dan malam hari tanpa menggunakan *blitz* dan mengekspos posisi kamera. Namun, permasalahan dalam penggunaan gambar termal untuk pengenalan wajah adalah, basis data untuk pengenalan wajah masih terbatas. Diego Socolinsky dan Andrea Selinger (2004) meneliti penggunaan pengenalan wajah termal dalam kehidupan nyata dan *operation sceneries*, dan pada saat yang sama membangun database baru gambar wajah termal. Penelitian ini menggunakan sensor listrik feroelektrik beresolusi rendah dan sensitif, yang mampu menangkap gelombang panas inframerah- *Long Wave Thermal Infrared* (LWIR).

Hasilnya menunjukkan bahwa perpaduan LWIR dan kamera visual biasa memiliki hasil yang lebih baik dalam penyelidikan di luar ruangan. Hasil dalam ruangan menunjukkan bahwa metode visual memiliki akurasi 97,05%, sedangkan LWIR 93,93%, dan gabungan 98,40%, namun pada luar ruangan, membuktikan metode visual memiliki 67,06%, LWIR 83,03%, dan metode gabungan memiliki 89,02%. Penelitian ini menggunakan 240 subjek selama 10 minggu untuk membuat database baru. Data dikumpulkan pada hari yang cerah, hujan, dan berawan.

Pada tahun 2018, para peneliti dari Laboratorium Penelitian Angkatan Darat A.S. mengembangkan teknik yang memungkinkan mereka untuk mencocokkan citra wajah yang diperoleh menggunakan kamera termal dengan citra wajah yang ada di basis data yang ditangkap menggunakan kamera konvensional. Pendekatan ini menggunakan kecerdasan buatan *Artificial Intelligence* (AI). Dikenal sebagai metode sintesis lintas-spektrum

karena cara ini menjembatani pengenalan wajah dari dua modalitas pencitraan yang berbeda.

Para ilmuwan ARL telah mencatat bahwa pendekatan ini bekerja dengan menggabungkan informasi global (mis. Fitur di seluruh wajah) dengan informasi lokal (mis. Fitur mengenai mata, hidung, dan mulut). Selain untuk meningkatkan pembedaan gambar yang disintesis, sistem pengenalan wajah dapat digunakan untuk mengubah tanda tangan wajah termal menjadi gambar wajah yang halus. Menurut tes kinerja yang dilakukan di ARL, para peneliti menemukan bahwa model sintesis lintas-spektrum multi-wilayah, menunjukkan peningkatan kinerja sekitar 30% dibandingkan metode awal dan sekitar 5% dibandingkan metode canggih.

5. Aplikasi *Facial Recognition*

Platform media sosial telah mengadopsi kemampuan pengenalan wajah untuk mendiversifikasi fungsi mereka guna menarik basis pengguna yang lebih luas di tengah persaingan ketat dari berbagai aplikasi. Didirikan pada tahun 2013, Looksery terus mengumpulkan uang untuk aplikasi modifikasi wajahnya di Kickstarter. Setelah pengumpulan dana berhasil, Aplikasi Looksery diluncurkan pada Oktober 2014. Aplikasi ini memungkinkan obrolan melalui video melalui filter khusus untuk wajah, yang mengubah tampilan pengguna. Meskipun ada aplikasi penambahan gambar seperti FaceTune dan Perfect365, mereka hanya terbatas pada gambar statis, sedangkan Looksery memungkinkan *augmented reality* untuk video langsung.

Pada akhir tahun 2015, SnapChat membeli aplikasi Looksery. Lensa animasi SnapChat, yang menggunakan

teknologi pengenalan wajah, merevolusi dan mendefinisikan ulang selfie, dengan memungkinkan pengguna menambahkan filter untuk mengubah penampilannya. Pilihan filter berubah setiap hari, beberapa contoh termasuk yang membuat pengguna terlihat seperti versi tua dan kusut, dan yang menempatkan mahkota bunga virtual di atas kepala mereka. Filter anjing adalah filter paling populer yang membantu mendorong kesuksesan berkelanjutan SnapChat, dengan selebritis populer seperti Gigi Hadid, Kim Kardashian, dll. yang secara teratur memposting video diri mereka dengan filter anjing. DeepFace adalah sistem pengenalan wajah yang dibuat oleh kelompok riset di Facebook.

Sistem ini mengidentifikasi wajah manusia dalam gambar digital. Sistem ini menggunakan jaringan saraf sembilan lapis dengan lebih dari 120 juta koneksi, dan diuji coba pada empat juta gambar yang diunggah oleh pengguna Facebook. Sistem ini dikatakan 97% akurat, dibandingkan dengan 85% untuk sistem Identifikasi Generasi terbaru FBI. Salah satu pencipta perangkat lunak ini, Yaniv Taigman, datang ke Facebook melalui akuisisi mereka terhadap Face.com. Penggunaan pengenalan wajah yang muncul saat ini adalah penggunaan layanan verifikasi ID. Banyak perusahaan sekarang yang menyediakan layanan ini kepada pihak perbankan, ICO, dan bisnis elektronik lainnya. Apple memperkenalkan Face ID pada iPhone X, sebagai pengganti otentikasi biometrik untuk Touch ID (sistem berbasis sidik jari). Face ID memiliki sensor pengenalan wajah yang terdiri dari dua bagian: modul "Romeo" yang memproyeksikan lebih dari 30.000 titik inframerah ke wajah pengguna, dan modul "Juliet" yang membaca polanya. Pola tersebut dikirim ke "*Secure*

Enclave" di *Central Processing Unit* (CPU) perangkat untuk mengonfirmasi kecocokan dengan wajah pemilik ponsel. Pola wajah yang tersimpan di perangkat, tidak dapat diakses oleh Apple. Sistem tidak akan bekerja dengan mata tertutup, dalam upaya untuk mencegah akses tidak sah. Teknologi ini belajar dari perubahan penampilan pengguna, dan karenanya bekerja dengan topi, syal, kacamata, dan banyak kacamata hitam, janggut dan rias wajah. Teknologi ini juga berfungsi dalam gelap, dilakukan dengan menggunakan "Flood Illuminator" (lampu kilat inframerah khusus) yang mengeluarkan cahaya inframerah yang tidak terlihat ke wajah pengguna untuk membaca dengan benar 30.000 titik wajah.

C. Biometrik Telapak Tangan

Sistem pengenalan diri merupakan sebuah sistem yang dapat digunakan untuk mengenali identitas seseorang yang dapat dilakukan secara otomatis menggunakan komputer [1]. Sistem pengenalan diri pada umumnya telah banyak menggunakan kata sandi (password), ID card, atau PIN untuk mengenali identitas seseorang [2]. Permasalahan yang sering muncul yaitu, pengenalan diri dengan sistem tersebut memiliki beberapa kelemahan diantaranya, penggunaan PIN maupun password memiliki kelemahan bahwa seseorang kerap kali lupa akan password yang mereka miliki dan beberapa password dapat dengan mudah di perkirakan oleh orang-orang yang tidak bertanggung jawab [3]. Oleh karena itu dengan adanya biometrika sangat membantu dalam menyelesaikan permasalahan-permasalahan yang muncul dalam sistem pengenalan diri [1][2][3]. Sistem pengenalan diri secara otomatis sangat di butuhkan di era informasi seperti sekarang ini [1]. Pengenalan diri secara otomatis

dapat dilakukan dengan menggunakan bagian tubuh atau perilaku manusia yang dikenal dengan istilah biometrika [4][5][6].

Biometrika merupakan teknologi pengenalan diri yang menggunakan bagian tubuh atau perilaku dari manusia [4]. Biometrika memiliki ciri kerja dengan mengukur karakteristik pembeda pada badan atau perilaku seseorang tersebut dengan membandingkan karakteristik yang sebelumnya telah disimpan pada suatu database [7]. Terdapat beberapa cara untuk biometrika umum yang sering dipakai untuk pengenalan diri, seperti sidik jari (*fingerprint*), selaput pelangi, (iris), wajah (*face*), suara (*voice*), tanda tangan (signature), geometri tangan (*hand geometry*) dan telapak tangan (*palmprint*) [8].

Telapak tangan (*palmprint*) merupakan salah satu bagian tubuh dari manusia yang memiliki nilai biometrika sehingga relatif baru untuk diteliti dan digunakan dalam sistem pengenalan [9]. Dari permukaan telapak tangan yang dimiliki oleh setiap orang diharapkan dapat menghasilkan ciri yang mampu membedakan masing-masing pemilik telapak tangan yang di identifikasi [10]. Penggunaan telapak tangan dalam proses pengenalan diri sangat banyak digunakan karena telapak tangan memiliki karakteristik yang unik, tidak mudah di palsukan dan cenderung stabil [9][10]. Dengan adanya karakteristik tersebut maka telapak tangan dapat digunakan sebagai alat verifikasi identitas seseorang dengan melakukan pencocokan data yang terdapat dalam sebuah database dengan data yang sudah di masukkan.

1. *Preprocessing*

Prepocessing merupakan suatu proses pengolahan citra yang dilakukan sebelum proses pengenalan pola (Suryani and Candra, 2018). *Prepocessing* yang dilakukan dalam

penelitian ini yaitu cropping, resizing, dan segmentasi citra. Berikut beberapa proses yang dilakukan pada tahap penelitian:

a. *Cropping* dan *Resizing*

   Cropping merupakan proses pengolahan citra yang di lakukan dengan dengan cara memotong suatu citra yang berfungsi untuk mengambil bagian penting dari citra tersebut (Suryani and Candra, 2018). Sedangkan Resizing merupakan proses pengolahan citra yang dilakukan untuk mengubah ukuran citra. Pada penelitian ini, citra tangan dicrop sesuai dengan objek telapak tangan.

2. Segmentasi Citra

Segmentasi citra merupakan tahapan penting dalam proses pengenalan pola yang bertujuan untuk memisahkan antara objek (*foreground*) dengan (*background*) (Suryani and Candra, 2018). Pada penelitian ini, segmentasi citra bunga dilakukan dengan menggunakan metode segmentasi citra dalam color space RGB.

3. Ekstraksi Fitur

Ekstraksi fitur merupakan proses untuk mengambil ciri atau informasi dari suatu objek dalam citra. Sedangkan fitur merupakan karakteristik unik dari suatu objek (Suryani and Candra, 2018). Dalam penelitian ini, ekstraksi fitur telapak tangan dilakukan dengan menggunakan metode PCA (*Principal Component Analysis*). Secara umum, tahapan proses ekstraksi fitur telapak tangan yang dilakukan yaitu

a. Mengkonversi citra telapak tangan RGB ke *grayscale* (citra 2D).

b. Mengimplementasikan algoritma PCA.
c. Menentukan banyak nilai PC yang akan digunakan sebagai variabel input dalam klasifikasi JST (Jaringan Syaraf Tiruan).

4. Klasifikasi

Klasifikasi merupakan proses pengelompokkan objek ke dalam kelas yang sesuai. Dalam penelitian ini, proses klasifikasi di lakukan untuk mengelompokkan telapak tangan berdasarkan fitur bentuk telapak tangan dengan menggunakan Metode Jaringan Syaraf Tiruan Backpropagation. Proses klasifikasi pada sistem perancangan ini terdiri dari 2 tahap, yaitu tahap pelatihan dan tahap pengujian.

a. Berikut proses klasifikasi pada tahap pelatihan :
   1) Menentukan variabel data input dan target pelatihan.
   2) Menentukan jumlah hidden layer dan jumlah neuron pada hidden layer.
   3) Membangun arsitektur jaringan.
   4) Menentukan nilai parameter JST yang mempengaruhi proses pelatihan.
   5) Melakukan pelatihan jaringan.
   6) Menghitung akurasi dan nilai MSE.

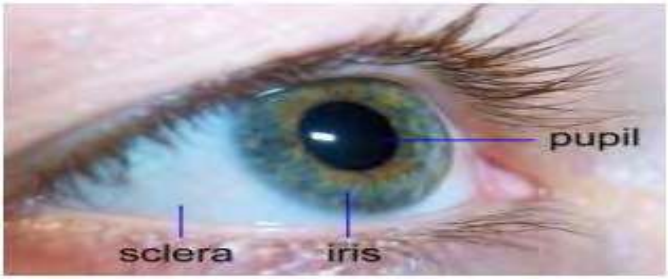
b. Berikut proses klasifikasi pada fase pengujian :
   1) Menentukan variabel data input.
   2) Memanggil jaringan yang telah dibangun pada proses pelatihan.
   3) Melakukan pengujian dan menghasilkan *output.*
   4) Menghitung nilai akurasi sistem pengenalan jenis telapak tangan.

D. Biometrik Iris

Iris biometrik mengidentifikasi manusia dengan pola iris yang diambil dari citra mata. Mata manusia terdiri 3 bagian utama : pupil (bagian yang berwarna hitam), iris(bagian yang berwarna) dan sclera (bagian yang berwarna putih). Radius dari batas dalam iris dengan pupil tidak tetap karena pupil akan melebar dan menyempit bergantung pada banyaknya cahaya yang masuk ke pupil. Pigmentasi pada iris manusia terdiri dari 2 molekul utama yaitu eumalin coklat-hitam (lebih dari 90%) dan pheomelanin kuning-kemerahan. Eumelanin menghasilkan emisi fluoresen yang paling banyak pada daerah cahaya tampak, yang memungkinkan untuk pengambilan citra dengan detail yang lebih banyak, namun juga lebih banyak noise yang didapat, termasuk akibat adanya pantulan teratur dan baur serta bayangan yang terbentuk. Sedangkan untuk cahaya NIR lebih umum digunakan karena mengurangi ketidaknyamanan akibat penyinaran langsung pada mata, dimana intensitas maksimum yang distandarkan sebesar 10 mW/cm 2[3].

Setiap individu mempunyai pola iris yang unik, tekstur visual dari iris terbentuk permanen saat berumur 2 tahun, tekstur pola iris yang kompleks membawa informasi yang menjanjikan untuk pengenalan seseorang. Pola ini dapat diekstraksi dari gambar mata yang kemudian dikodekan. Kode ini yang kemudian dibandingkan dengan kode yang didapatkan dari gambar mata lain dimana hasilnya akan menggambarkan perbedaan antara kode mata yang berbeda, atau dengan kata lain dapat disimpulkan bahwa pola mata yang dibandingkan akan sama atau berbeda. Untuk mendapatkan pengenalan iris yang akurat, segmentasi iris sangat diperlukan. dua metode yang dikenal untuk segmentasi iris

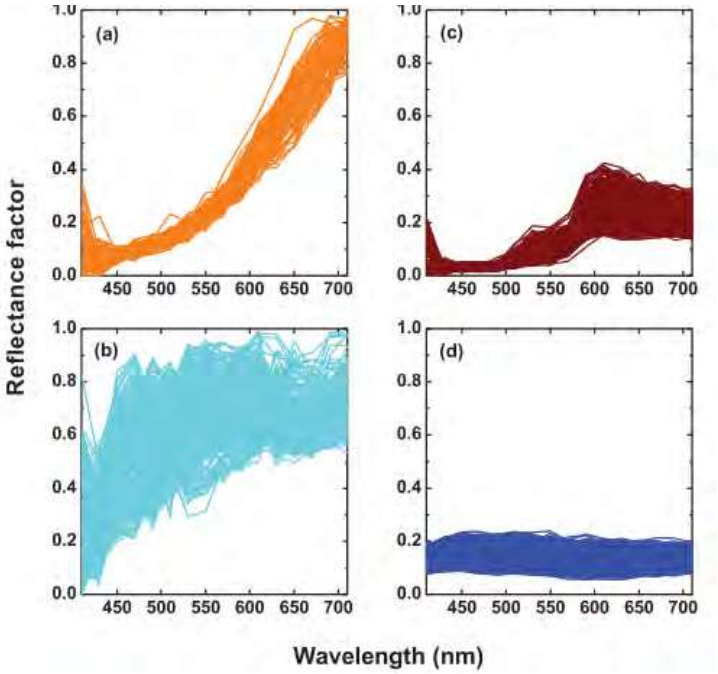
yaitu metode wilde dan metode daugman. Wilde mengenalkan 2 tahap segmentasi iris :



Gambar 4.1 Citra mata yang menggambarkan iris,pupil dan sclera (www.sternvision.com)

1. Membinerkan ujung citra berdasarkan *gradient* berdasarkan terbentuknya intensitas piksel pada citra iris, batas bagian dalam dan luar iris dideteksi dengan *Hough Transform*. Algoritma daugman, dinamakan dari professor John Daugman, merupakan operator integrodifferensial yang mencari lingkaran pupil dan batas iris pada keseluruhan citra. Algoritma ini merupakan detektor ujung lingkaran yang mencari parameter dari batas-batas lingkaran.
2. Penjumlahan dari keliling nilai intensitas pixel pada batas lingkaran merupakan perubahan nilai maksimum dibandingkan 1 daerah piksel dengan radius yang lebih jauh dari pusat piksel yang sama[5]. Medina, dkk. [6], melalui penelitianya mengenai reflektansi iris manusia yang diambil secara in vivo, mengkategorikan reflektansi mata berdasarkan pigmen iris gelap (oranye), cerah (cyan), gelap(merah-gelap) dan cerah(biru tua) dimana reflektansi minimum berada pada daerah dengan panjang gelombang di bawah 430 nm dan mulai meningkat sampai

700 nm. Hasil ini memungkinkan dilakukan pengambilan citra iris pada panjang gelombang 550 nm ke atas.

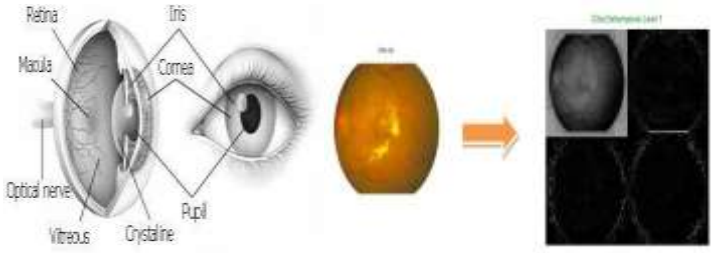


Gambar 4.2. Reflektansi iris dengan warna pigmen (a) gelap (oranye), (b) cerah (cyan), (c) gelap (merah tua) dan (d) cerah (biru tua).

E. Biometrik Retina

Retina adalah selapis tipis sel yang terletak pada bagian belakang bola mata vertebrata dan sefalopoda. Retina merupakan bagian mata yang mengubah cahaya menjadi sinyal saraf. Struktur retina manusia adalah 72% seperti bola dengan diameter sekitar 22 mm. Pada bagian tengah retina terdapat cakram optik, yang dikenal sebagai "titik buta" (blind spot) karena tidak adanya fotoreseptor di daerah itu. Cakram optik terlihat sebagai area oval berwarna putih berukuran 3

mm^2 Gambar 2.1 adalah anatomimata yang menunjukkan letak retina mata berada.



Gambar 4.3. Anatomi mata (Moreno *et al.,* 2009)

F. Biometrik Suara

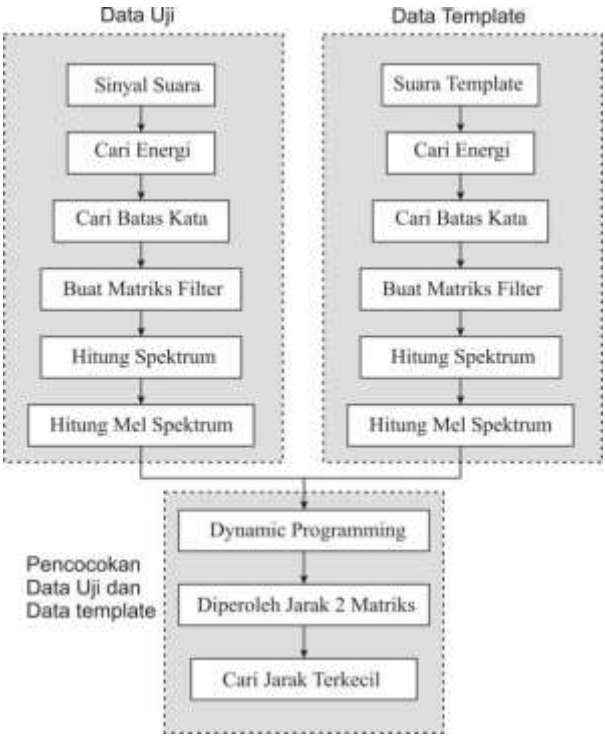
Suatu ucapan dapat dibedakan apakah tergolong ucapan pernyataan (*declarative*) atau pertanyaan (*interrogative*) hanya melalui intonasinya [8]. Perbedaan intonasi akan menggambarkan perbedaan informasi yang disampaikan oleh pembicara. Ketika kita mendengar sebuah ucapan "kamu sudah makan", maka kemungkinan pendengar akan menangkap sebuah ucapan pernyataan ataupun sebuah pertanyaan. Sudah pasti dengan intonasi berbeda akan menyebabkan tanggapan yang diterima oleh pendengar juga akan berbeda. Pendeteksian intonasi telah dilakukan oleh beberapa peneliti, terutama untuk intonasi Bahasa Inggris. Suatu ucapan terdiri dari satu atau lebih bagian-bagian intonasi [8]. Parameter yang digunakan untuk melihat fenomena intonasi adalah pitch.

Penelitian tentang pitch dilakukan dengan menganalisis kontur frekuensi fundamental (F0 contours) dari sebuah ucapan. Di sisi lain, pencarian pitch yang lebih teliti dilakukan dengan mempertimbangkan efek laringealisasi (*laryngealiza-*

tion effects). Efek ini tergambarkan sebagai eksitasi suara yang tidak teratur. Hal ini disebabkan oleh sinyal suara yang memiliki periodisitas yang tidak reguler, memiliki variasi amplitudo yang besar, atau memiliki periode pitch yang terlalu lama [8]. Estimasi terhadap frekuensi fundamental atau yang dikenal dengan deteksi pitch, merupakan topik yang sangat populer untuk diteliti dalam beberapa tahun, bahkan sampai saat ini.

Masalah dasar dalam mengekstraksi frekuensi fundamental (fo) dari suatu gelombang suara adalah pencarian bagian-bagian komponen gelombang yang memiliki frekuensi terendah. Suatu bagian-bagian (*partials*) gelombang akan terkait dengan bagian lainnya [9]. Bagian terendah (*first partial*) adalah frekuensi fundamental (fo) dari suatu gelombang suara. Wardana (2008) telah membuat aplikasi untuk membedakan antara intonasi pernyataan (*declarative*) dan intonasi pertanyaan (*interrogative*) hanya melalui intonasinya untuk melakukan system kontrol dan *monitoring* penggunaan perangkat listrik [10]. Sistem yang dibangun menggunakan jaringan saraf tiruan untuk membedakan kedua intonasi tersebut, dan proses pengolahan suara memanfaatkan MATLAB pada aplikasi desktop.

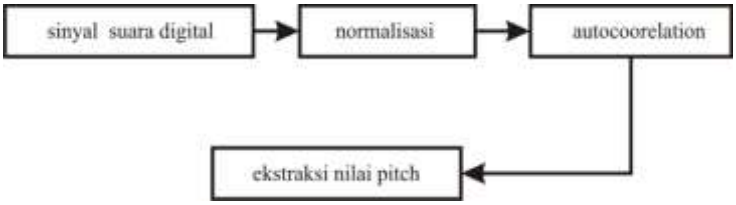
Namun demikian, penggunaan aplikasi desktop untuk beberapa kasus menjadi kurang efisien, sebagai contoh penerapan sistem keamanan untuk akses pintu. Penggunaan komputer desktop dirasa akan menghabiskan sumber daya listrik yang cukup besar, terutama jika system digunakan sepanjang hari. Oleh karena itu, pada penelitian ini, penulis mencoba mengganti aplikasi desktop dengan sebuah mikrokomputer, dan selanjutnya meneliti keandalan sistem.



Gambar 4.4. Diagram Alir Sistem Pengenalan Suara

Program pengenalan intonasi dilakukan dengan mengekstrak nilai frekuensi fundamental (F0) dari suatu ucapan. Nilai F0 dianggap mewakili kontur intonasi (*pitch*). Metode yang digunakan untuk mencari frekuensi fundamental adalah metode autokorelasi dan jaringan saraf tiruan (JST). Metode autokorelasi diperlihatkan pada Gambar 4. Nilai-nilai frekuensi fundamental dari proses autokorelasi akan menjadi input untuk jaringan saraf tiruan, baik sebagai data latih maupun data uji. Agar sistem identifikasi terhadap jenis intonasi dapat dilakukan, maka sebelumnya dilakukan pembuatan database intonasi, ekstraksi nilai pitch, dan pemrograman jaringan

saraf tiruan. Jaringan saraf tiruan memerlukan data latih dan data uji berupa sampel suara. Berbagai sampel suara yang dilatih akan menentukan tingkat kecerdasan jaringan untuk mengenali pola-pola yang belum diketahuinya, dalam hal ini untuk membedakan suatu intonasi. Jaringan yang dibangun akan dicoba menggunakan input berupa nilai pitch suara. Melalui pemrograman, akan dicari metode pelatihan (training) yang paling tepat dalam pengenalan jaringan terhadap pola-pola input. Pencarian jumlah neuron lapisan tersembunyi juga akan dilakukan, agar error yang dihasilkan output seminimal mungkin.



Gambar 4.5. Metode Autokorelasi

Jaringan saraf tiruan memerlukan data latih dan data uji berupa sampel suara. Berbagai sampel suara yang dilatih akan menentukan tingkat kecerdasan jaringan untuk mengenali pola-pola yang belum diketahuinya, dalam hal ini untuk membedakan suatu intonasi. Jaringan yang dibangun akan dicoba menggunakan input berupa nilai *pitch* suara. Melalui pemrograman, akan dicari metode pelatihan (*training*) yang paling tepat dalam pengenalan jaringan terhadap pola-pola input. Pencarian jumlah neuron lapisan tersembunyi juga akan dilakukan, agar error yang dihasilkan *output* seminimal mungkin.

G. Biometrik Tanda tangan

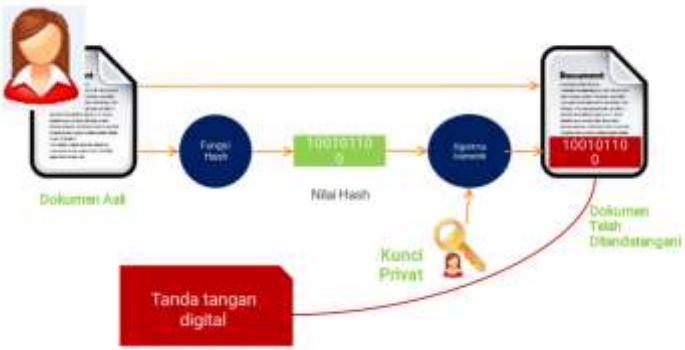
Digital *signature,* di Indonesia itu ada beberapa peringkat. Yakni terdaftar, lalu tersertifikasi, dan berinduk. Kalau berinduk, platform harus memenuhi banyak persyaratan teknis, sistem, dan keamanan yang harus dilakukan. Selain harus lolos audit yang cukup ketat dari Kementerian Kominfo, status tersebut turut didapat perusahaan berkat infrastruktur yang tersertifikasi. Misalnya, mereka sudah mendapatkan ISO 27001 untuk keamanan sistem. Perusahaan juga telah memiliki fasilitas pusat data tier-3 dan pusat pemulihan data tier-4 untuk melakukan proses bisnis. TekenAja juga diklaim menjadi penyedia *platform* tanda tangan digital pertama yang benar-benar memanfaatkan verifikasi biometrik. Untuk validasi data, mereka telah menjalin perjanjian kerja sama dengan Dukcapil untuk mengakses data kependudukan.

"Biasanya ketika melakukan verifikasi identitas, pengguna akan diminta selife bersama KTP-nya. Kemudian sistem akan mencocokkan foto yang ada di KTP dengan wajah aslinya. Mekanisme tersebut masih memiliki celah, pengguna yang tidak bertanggung jawab bisa saja menggunakan identitas (NIK, nama, alamat, dll.) orang lain, kemudian membuat KTP palsu dengan fotonya sendiri untuk verifikasi. Maka dari itu biometrik menjadi penting," lanjut Rionald. Ia juga menjelaskan, konsep tanda tangan digital ini pada dasarnya memungkinkan individu untuk bisa melakukan transaksi online secara aman dengan melampirkan sertifikat digital (berisi data pribadi) yang telah terverifikasi.

Gambar 4.6. Model Tanda Tangan Digital

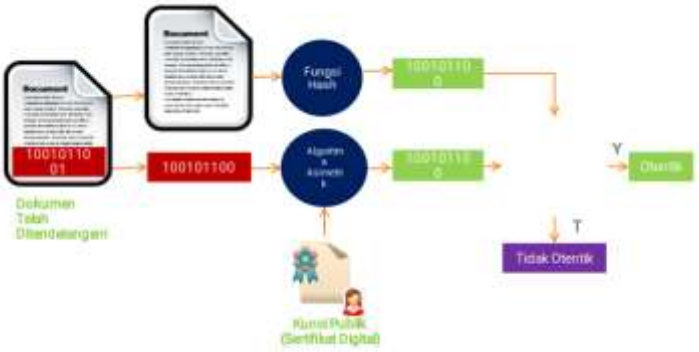
Keluarannya bisa bermacam-macam, beberapa yang populer berupa tanda tangan elektronik atau kode QR unik. Peran pemain seperti TekenAja tugasnya melakukan penerbitan sertifikat digital tersebut. "*Digital signature* cakupannya sampai harus memverifikasi identifikasinya. Ada beberapa tahapan, waktu pendaftaran orangnya harus benar. Kemudian ketika melakukan proses transaksi, juga harus diverifikasi. Jadi katakanlah istri saya punya data login saya untuk menandatangani sesuatu, dia tetap tidak bisa menggunakan karena harus diverifikasi dulu biometriknya untuk memastikan yang tanda tangan benar-benar saya.

Untuk pengguna akhir, layanan TekenAja saat ini bisa dipakai di lembaga jasa keuangan untuk menjaga transaksi bisa berjalan secara online dan aman. Pengguna nantinya bisa menggunakan aplikasi mobile untuk melakukan proses tanda tangan. Tapi tidak hanya menutup di sektor itu saja, nantinya juga akan diperluas kegunaannya untuk fungsi-fungsi lain. Contohnya membantu sistem HRD di perusahaan agar berbagai pengajuan (cuti, *reimbursement*, dll.) yang dilakukan karyawan pengesahannya dilakukan secara digital.



Gambar 4.7. Proses Tanda Tangan Digital

Di sisi bisnis nantinya akan ada dua model penerapan, bisa melalui portal khusus yang disediakan atau melalui integrasi API ke dalam sistem aplikasi. Sementara yang sudah pakai TekenAja ada perbankan, multi-finansial, fintech, hingga perusahaan ritel. ionald mengatakan, penerapan TekenAja bakal bisa digunakan untuk menjamin legalitas transaksi antarindividu. Ia mencontohkan, ketika ada akad jual-beli mobil atau rumah, pengesahannya (biasanya dilakukan dengan tanda tangan basah di atas materai) bisa dilakukan secara digital lewat aplikasi. Platform autentikasi biometrik Asli RI dan Login ID. Dengan induk perusahaan yang sama, TekenAja pun terintegrasi dengan kapabilitas yang dimiliki Asli RI. "TekenAja adalah perusahaan digital signature yang kental dengan biometrik. Karena menurut saya autentikasi biometrik itu saat ini jadi sistem keamanan terbaik, paling sulit dijebol. Pemerintah Indonesia baik itu Dukcapil maupun Kominfo cukup suportif dalam hal penerapan biometrik untuk tanda tangan digital.



Gambar 4.8. Proses Verifikasi Tanda Tangan Digital

Gambar 4.9. Proses Verifikasi Tanda Tangan Digital

H. Biometrik Cara pengetikan

Password bisa disebut sebagai milik pribadi yang paling berharga, karena password memegang peranan dalam kehidupan sehari-hari, seperti pada saat menggunakan ATM, mengakses e-mail, dan sebagainya. Begitu pentingnya password, sehingga apabila password diketahui oleh orang lain, maka dapat diperkirakan akibat yang akan terjadi. *Keystroke dynamics* adalah biometrik yang memverifikasi

seorang user berdasarkan irama pengetikan. Metode yang dipakai adalah statistik yakni dengan membandingkan pengetikan pada saat login dengan profil pengetikan yang tersimpan sebelumnya. Dengan adanya keystroke dynamics maka mampu menjamin keamanan data, karena di samping identifikasi yang dilakukan terhadap password yang diketik sekaligus juga dilakukan verifikasi terhadap irama pengetikan. Pada masa sekarang ini banyak sekali suatu pekerjaan yang tidak terlepas dari kegiatan tulis menulis. Pada jaman dahulu kita dapat menggunakan sebuah alat bantu yaitu mesin ketik, dimana seiring dengan pekembangan jaman telah ditemukan sebuah alat bantu yang lebih modern yang kita sebut komputer. Penggunaan komputer di Indonesia khususnya dalam kegiatan tulis menulis sudah berkembang diberbagai bidang, baik dibidang pendidikan, dan junalis. Perkembangan kegiatan tulis menulis didunia pendidikan dan junalis tidak terlepas dari penggunaan alat bantu yang berupa software-software word prosesing yang makin lama makin canggih dan mudah dalam penggunaannya. Walaupun software yang digunakan makin namun software -software yang ada tersebut masih kuang interaktif dan masih sulit digunakan bagi beberapa orang

terutama orang-orang yang mengalami masalah pada penglihatannya. Maka dari itu penulis kali ini akan mencoba membuat suatu software yaitu Teks Editor yang sederhana yang dapat memudahkan pengguna text editor terutama orang-orang yang mengalami masalah pada penglihatannya untuk melakukan tugasnya yaitu proses kegiatan tulis menulis, dimana pada Teks Editor ini penggunannya akan mendapatkan panduan yang berupa suara dari kata yang mereka ketikan. Dimana proses itu biasa disebut Teks To Speech.

1. *Text To Speech*

Text to Speech (TTS) diartikan sebagai proses pengubahan teks menjadi audio digital dan diucapkan. Pengucapan ini dapat berupa pengiriman audio digital tersebut ke pengeras suara komputer atau menyimpan hasil pengubahan tersebut untuk diputar nanti. Dalam mengubah teks menjadi audio, *TTS engine* menggunakan bermacam-macam metode, antara lain:

a. Penggabungan frasa kata
b. Sitesis kata
c. Penggabungan frasa kata dan sintesis kata

TTS engine yang digunakan dalam aplikasi Teks Editor menggunakan metode ketiga yaitu penggabungan frasa kata dan sintesis kata.

a. Penggabungan Frasa Kata

Metode ini menggabungkan frasa kata yang sebelumnya telah direkam untuk membentuk sebuah kalimat dan merupakan metode yang paling mudah serta paling banyak digunakan saat ini. Kebanyakan *system voice-mail* menggunakan metode ini. Sebagai contoh, pesan pada *voice-mail* "Anda mempunyai [dua] buah pesan", ini merupakan pesan yang terdiri dari tiga bagian yaitu dua buah pesan yang bersifat statis "Anda mempunyai" dan "buat pesan" serta sebuah pesan yang bersifat dinamis tetapi telah dipersiapkan sebelumnya yaitu "dua".

b. Sintesis Kata

Metode ini menghasilkan sintesis atau tiruan kata secara elektronik dengan menerapkan algoritma perhitungan yang kompleks untuk mensimulasikan pita suara, rongga mulut, bentuk bibir dan posisi lidah.

Suara yang dihasilkan dari metode ini seperti suara robot tetapi dengan algoritma yang telah ada pada *Text to Speech engine* menjadi seperti suara manusia.

c. *Penggabungan Frasa Kata dan Sintesis Kata*
Metode ini menggabungkan segmen audio dan menggunakan algoritma perhitungan untuk menghaluskan jeda guna menghasilkan suara yang utuh. Contohnya adalah "hello", terdiri dari empat segmen.

2. Konversi dari Teks ke Ucapan

Sistem *Text to Speech* pada prinsipnya terdiri dari dua sub sistem, yaitu

a. Bagian Konverter Teks ke Fonem (*Text to Phoneme*), serta
b. Bagian Konverter Fonem ke Ucapan (*Phoneme to Speech*).

Bagian Konverter Teks ke Fonem berfungsi untuk mengubah kalimat masukan dalam suatu bahasa tertentu yang berbentuk teks menjadi rangkaian kode-kode bunyi yang biasanya direpresentasikan dengan kode fonem, durasi serta *pitch*-nya. Bagian ini bersifat sangat language dependant. Untuk suatu bahasa baru, bagian ini harus dikembangkan secara lengkap khusus untuk bahasa tersebut.

Bagian Konverter Fonem ke Ucapan akan menerima masukan berupa kode-kode fonem serta *pitch* dan durasi yang dihasilkan oleh bagian sebelumnya. Berdasarkan kode-kode tersebut, bagian Konverter Fonem ke Ucapan akan menghasilkan bunyi atau sinyal ucapan yang sesuai dengan kalimat yang ingin diucapkan. Ada beberapa alter-

natif teknik yang dapat digunakan untuk implementasi bagian ini. Dua teknik yang banyak digunakan adalah *formant synthesizer*, serta *diphone concatenation*. *Formant synthesizer* bekerja berdasarkan suatu model matematis yang akan melakukan komputasi untuk menghasilkan sinyal ucapan yang diinginkan. *Synthesizer* jenis ini telah lama digunakan pada berbagai aplikasi. Walaupun dapat menghasilkan ucapan dengan tingkat kemudahan interpretasi yang baik, *synthesizer* ini tidak dapat menghasilkan ucapan dengan tingkat kealamian yang tinggi.

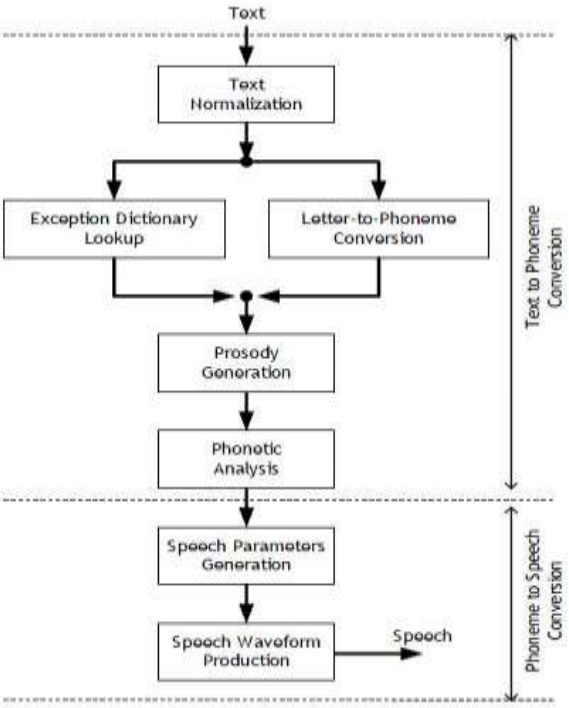
Synthesizer yang menggunakan teknik *diphone concatenation* bekerja dengan cara menggabung-gabungkan segmen-segmen bunyi yang telah direkam sebelumnya. Setiap segmen berupa *diphone* (gabungan dua buah fonem). *Synthesizer* jenis ini dapat menghasilkan bunyi ucapan dengan tingkat kealamian (*naturalness*) yang tinggi. Struktur sistem seperti di atas pada prinsipnya merupakan konfigurasi tipikal yang digunakan pada berbagai sistem *Text to Speech* berbagai bahasa.

Namun demikian, pada setiap sub-sistem terdapat sifat-sifat serta proses-proses yang sangat spesifik dan sangat tergantung dari bahasanya. Konversi dari teks ke fonem sangat dipengaruhi oleh aturan-aturan yang berlaku dalam suatu bahasa. Pada prinsipnya proses ini melakukan konversi dari simbol-simbol tekstual menjadi simbol-simbol fonetik yang merepresentasikan unit bunyi terkecil dalam suatu bahasa. Setiap bahasa memiliki aturan cara pembacaan dan cara pengucapan teks yang sangat spesifik.

Hal ini menyebabkan implementasi unit konverter teks ke fonem menjadi sangat spesifik terhadap suatu bahasa. Untuk mendapatkan ucapan yang lebih alami,

ucapan yang dihasilkan harus memiliki intonasi (*prosody*). Secara kuantisasi, prosodi adalah perubahan nilai *pitch* (frekuensi dasar) selama pengucapan kalimat dilakukan atau pitch sebagai fungsi waktu. Pada praktiknya, informasi pembentuk prosodi berupa data-data pitch serta durasi pengucapannya untuk setiap fonem yang dibang-kitkan. Nilai-nilai yang dihasilkan diperoleh dari suatu model prosodi. Prosodi bersifat sangat spesifik untuk setiap bahasa, sehingga model yang diperlukan untuk membangkitkan data-data prosodi menjadi sangat spesifik juga untuk suatu bahasa. Beberapa model umum prosodi pernah dikembangkan, tetapi untuk digunakan pada suatu bahasa masih perlu banyak penyesuaian yang harus dilakukan.

Konverter fonem ke ucapan berfungsi untuk mem-bangkitkan sinyal ucapan berdasarkan kode-kode fonem yang dihasilkan dari proses sebelumnya. Sub-sistem ini harus memiliki pustaka setiap unit ucapan dari suatu bahasa. Pada sistem yang menggunakan teknik *diphone concatenation,* sistem harus didukung oleh suatu *diphone* database yang berisi rekaman segmen-segmen ucapan yang berupa *diphone*. Ucapan dalam suatu bahasa dibentuk dari satu set bunyi yang mungkin berbeda untuk setiap bahasa, oleh karena itu setiap bahasa harus dilengkapi dengan *diphone* database yang berbeda. Tahapan-tahapan utama konversi dari teks menjadi ucapan dapat dinyatakan dengan diagram seperti terlihat pada Gambar 2.1 Tahap normalisasi teks berfungsi untuk mengubah semua teks kalimat yang ingin diucapkan menjadi teks yang secara lengkap memperlihatkan cara penguca- pannya. Lihat contoh kalimat dan hasil normalisasinya pada Gambar 2.2.



Gambar 4.10: Urutan Proses Konversi dari Teks ke Ucapan

Tahap berikutnya adalah melakukan konversi dari teks yang sudah secara lengkap merepresentasikan kalimat yang ingin diucapkan menjadi kode-kode fonem. Konversi teks menjadi fonem biasanya dilakukan dengan dua cara. Sebagian proses konversi dapat dilakukan dengan aturan konversi yang sederhana dan berlaku umum untuk berbagai kondisi. Sebagian proses lainnya bersifat kondisional, tergantung dari huruf-huruf atau fonem-fonem tetangganya, bahkan terdapat bentuk-bentuk translasi yang tidak dapat ditemukan keteraturannya. Konversi yang teratur dapat diimplementasikan dengan

table konversi yang berisi pasangan antara urutan huruf dan urutan fonem, bahkan mungkin hanya berisi satu huruf dan satu fonem. Aturan yang lebih sulit biasanya diimplementasikan dengan table konversi yang akan diterapkan jika kondisi rangkaian huruf tetangga kiri dan kanannya terpenuhi.

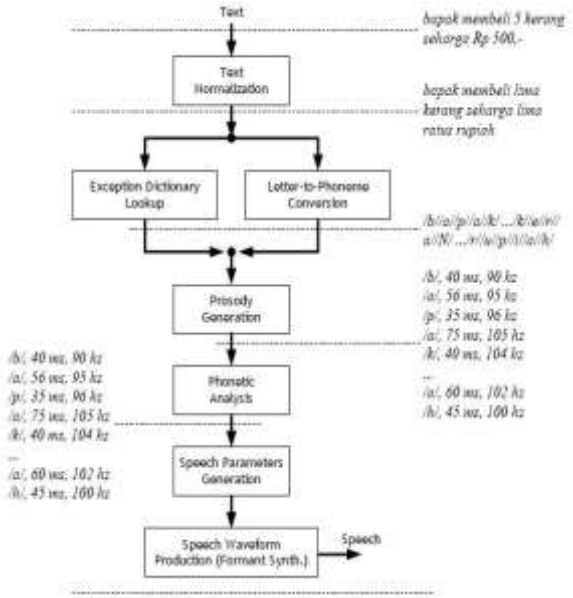
Contoh bentuk aturan konversi huruf ke fonem yang memenuhi teknik tersebut adalah sebagai berikut. Left-context [letter-set] right-context = phoneme string Huruf tertentu yang ditunjuk dalam posisi [letter-set] akan dikonversikan menjadi suatu fonem dalam "phoneme string" jika left-context dan right context terpenuhi. Bahasa Inggris termasuk bahasa yang mempunyai keteraturan yang rendah untuk proses konversi teks ke fonem.

Suatu TTS bahasa Inggris biasanya dilengkapi dengan suatu basis data yang berisi ribuan kata serta konversi padanan urutan fonemnya. Bahasa Indonesia termasuk bahasa yang jelas aturan konversinya. Sebagian besar kata dalam Bahasa Indonesia dapat dikonversikan menjadi fonem dengan aturan yang jelas dan sederhana, walaupun tetap ada kondisi-kondisi yang tidak dapat ditemukan keteraturannya.

Sebagai contoh, simbol huruf e dapat diucapkan sebagai e pepet atau etaling, artinya harus dikonversikan menjadi fonem yang berbeda untuk kondisi yang berbeda. Dalam blok diagram di atas, kondisi yang masih dapat ditangani oleh aturan diimplementasikan dengan blok *Letter to Phoneme Conversion*. Konversi yang tidak teratur ditangani oleh bagian *Exception Dictionary Lookup*. Hasil dari tahap tersebut adalah rangkaian fonem yang merep-resentasikan bunyi kalimat yang ingin diucapkan.

Bagian *prosody generator* akan melengkapi setiap unit fonem yang dihasilkan dengan data durasi pengucapannya serta *pitch*-nya. Data durasi serta *pitch* diperoleh berdasarkan kombinasi antara table atau database serta model prosodi. Secara simbolik, hasil dari bagian ini sudah menghasilkan informasi yang cukup untuk menghasilkan ucapan yang diinginkan. Satu tahap berikutnya yang masih sering dilakukan adalah *Phonetic Analysis*.

Tahap ini dapat dikatakan sebagai tahap penyempurnaan, yaitu melakukan perbaikan di tingkat bunyi. Sebagai contoh, dalam bahasa Indonesia, fonem /k/ dalam kata bapak tidak pernah diucapkan secara tegas, atau adanya sisipan fonem /y/ dalam pengucapan kata alamiah antara fonem /i/ dan /a/.



Gambar 4.11. Besaran-Besaran dalam Setiap Tahap Proses Konversi dari Teks ke Ucapan (dimodifikasi dari Pelton, 1992)

05 Penerapan Teknologi Biometrik untuk Keamanan Ruangan Rahasia

Peningkatan signifikan ketergantungan manusia pada sistem teknologi informasi telah menghasilkan sesuatu yang lebih besar yaitu jumlah data yang dihasilkan. Selain upaya bisnis dan profesional, banyak juga data digital yang dihasilkan dari kegiatan pribadi. Fakta terkait membuktikan bahwa 90% dari semua data yang ada saat ini diperoleh dalam dua tahun terakhir. Bangkitnya perangkat digital dan cerdas juga berkontribusi signifikan terhadap pertumbuhan data digital. Namun seiring dengan semua kenyamanan dan peningkatan efisiensi, ancaman terhadap keamanan data dan privasi juga meningkat. Di sisi lain, pengaruh teknologi biometrik yang meningkat untuk aplikasi identifikasi dan kontrol akses dipandang sebagai masa depan dari manajemen identitas.

Gambar 5.1. Konsep Keamanan Biometrik

Dalam beberapa tahun terakhir, teknologi biometrik telah muncul sebagai Cara yang menjanjikan untuk identifikasi manusia dan kontrol akses digital maupun akses fisik. Teknologi biometric ini menggunakan karakteristik anatomi atau perilaku manusia untuk proses identifikasi. Sistem yang didasarkan pada teknologi biometrik ini dapat menggunakan pengidentifikasi biometrik tunggal (seperti sidik jari) atau beberapa (profil biometrik perilaku) untuk proses identifikasi. Pengenalan dengan teknologi biometrik telah maju untuk beberapa modalitas seperti sidik jari, iris, wajah, tanda tangan, telapak tangan, retina, suara, dan DNA yang terus dikembangkan lebih luas sampai pengenalan gaya berjalan.

Gambar 5.2. Proses dalam Biometrik

Teknologi biometrik telah membantu orang mengganti metode identifikasi manusia dan kontrol akses yang lebih tua, tidak efisien, dan tidak nyaman seperti kunci pintu, dokumen identitas, kata sandi, pertanyaan keamanan, dan kerepotan yang terkait dengannya. Sebagian besar perangkat komputasi saat ini memasukkan identifikasi biometrik sebagai fitur yang harus dimiliki untuk menghilangkan keamanan berbasis kata

sandi. Platform *smartphone* utama seperti android, iOS, Windows, dan lain-lain menawarkan dukungan asli untuk memproses data biometrik dan kompatibilitas ke perangkat keras biometrik. Karena penyebaran luas dan efisiensinya, biometrik dipandang sebagai masa depan identifikasi manusia.

A. Keamanan Data Berbasis Kata Sandi Tidak Lagi Relevan

Meskipun biometrik telah digunakan di banyak bidang untuk keamanan data, sebagian besar masih bergantung pada keamanan berbasis kata sandi. Kata sandi telah ada sejak awal komputasi dan telah melayani tujuan manusia dengan sangat baik hingga beberapa tahun terakhir. Di lingkungan perusahaan, adanya kata sandi yang lemah, kebijakan yang tidak tepat, dan sikap ceroboh terhadap keamanan komputer dan jaringan dapat menyebabkan pelanggaran data. Serangan *ransomware WannaCry* yang terkenal pada Mei 2017 menunjukkan kepada dunia bagaimana ketidakmampuan organisasi untuk mengatasi kerentanan yang diketahui dari sistem operasi Windows mengakibatkan operasi dan kerugian terhenti. Serangan itu diperkirakan menginfeksi sebanyak 200.000 komputer dan beberapa organisasi menderita kerugian. Jika kita melihat daftar pelanggaran data Wikipedia, yang terdiri dari pelanggaran data yang dikonfirmasi terjadi sejak 2004-2021, terdapat beberapa alasan seperti berikut:

1. Data Pribadi/Rahasia tidak sengaja dipublikasikan
2. Dihasilkan dari peretasan
3. Dalam pekerjaan
4. Karena komputer yang hilang atau dicuri
5. Karena media yang hilang atau dicuri
6. Keamanan buruk
7. Rekayasa Sosial

Sayangnya, serangan *cyber* saat ini menjadi begitu rumit sehingga mungkin diperlukan waktu bertahun-tahun untuk mengetahui bahwa suatu pelanggaran telah terjadi bahkan mungkin sama sekali tidak bisa dilacak dalam beberapa kasus.

B. Krisis Keamanan Data Perbankan

Layanan perbankan dan keuangan selalu menjadi salah satu target utama penipu. Ketika semua bank terhubung dan dapat diakses melalui internet, layanan perbankan dan keuangan juga rentan terhadap penipuan *online* dan kejahatan dunia maya. Bank penargetan memiliki manfaat ganda bagi penjahat *cyber*:

1. Bank berurusan dengan uang yang bisa mencuri penjahat *cyber*.
2. Bank juga menyimpan informasi keuangan serta pribadi pelanggan.

Peretas dapat menghindari sistem otentikasi transaksi perbankan dengan berbagai cara. Dalam kasus *skimmers* ATM bekerja misalnya, penipu terus merekam detail kartu ATM serta tindakan pengguna pada perangkat yang ditindih pada tombol ATM dan pembaca kartu. Namun dalam hal perbankan *online*, peretas dapat menggunakan serangan canggih, pembajakan sesi, *malware* yang dibuat khusus untuk industri perbankan dan lain sebagainya. Industri perbankan dapat lebih sensitif daripada banyak jenis industri lainnya dan membutuhkan metodologi keamanan data yang canggih.

Enkripsi ujung ke ujung, *tokenization*, DLP (Pencegahan Kehilangan Data) merupakan beberapa teknologi yang diadopsi oleh bank untuk menerapkan keamanan dan privasi data. Bahkan hari ini, sebagian besar transaksi perbankan dan keuangan yang dilakukan pada *smartphone* dijamin dengan faktor otentikasi berbasis pengetahuan. Sebelum melakukan

transaksi, perangkat ini mencari otentikasi pengguna akhir sebagai konfirmasi. Konfirmasi ini secara tradisional dapat menggunakan PIN, kata sandi dan OTP. Ironisnya, sebagian besar perangkat ini sudah memiliki kemampuan biometrik seperti sidik jari atau pengenalan wajah.

C. Bisakah Biometrik Memecahkan Krisis Keamanan Data?

Salah satu keharusan mendasar dari keamanan data adalah bahwa data hanya boleh diakses oleh entitas yang berwenang. Ketika keamanan data diletakkan dengan kata sandi, sistem TI akan membiarkan siapa saja dengan kata sandi yang benar. Sayangnya sistem TI dapat dengan mudah dilacak karena mereka hanya mengenali informasi yang diberikan kepada mereka dan bukan pengguna. Bahkan orang yang tidak berwenang dengan kata sandi yang ditebak atau dicuri akan diperlakukan seperti orang yang berwenang dan tidak akan ada tindakan keamanan tambahan untuk menghentikannya.

Keamanan berbasis biometrik memperbaiki kelemahan mendasar ini dengan mengenali pengguna dengan sesuatu yang tidak dapat diubah atau ditiru dengan mudah: sifat fisiologis atau perilaku uniknya sendiri, yaitu pengidentifikasi biometrik. Kata sandi, terutama yang lebih lemah, adalah alasan utama dibalik pelanggaran data dan insiden keamanan. Berikut ini adalah cara biometrik dapat membantu memecahkan krisis keamanan data: Menghilangkan kata sandi dalam kontrol akses logis. Karena kata sandi dapat ditebak, bahkan dipecahkan, menggantinya dengan biometrik pengguna seperti sidik jari atau pengenalan pembuluh darah dapat menghilangkan kemungkinan data diakses oleh orang yang tidak berwenang.

D. Internet Menyangkut Masalah Keamanan

Sejauh ini, informasi dicuri dari insiden keamanan data karena internet saat ini sebagian besar adalah "internet informasi". Teknologi informasi ingin mendigitalkan setiap usaha manusia namun belum terlihat potensi sebenarnya. Setelah revolusi digital dan internet, IoT atau *Internet of Things* akan menjadi hal besar berikutnya yang sudah memasuki tahap eksperimental yang merambah pada akses rumah dan bisnis. Dengan demikian, memiliki peralatan yang terhubung seperti peralatan rumah, kendaraan dan lain-lain yang dapat berkomunikasi dengan perangkat lain akan dapat dirasakan dalam waktu dekat. Misalnya, IoT menghubungkan lemari es pintar yang akan melacak barang yang disimpan di dalamnya dan akan mengirimi Anda informasi tentang kaleng bir Anda yang berada di bawah jumlah yang ditentukan. Pendingin udara pintar akan mulai mendinginkan rumah Anda secara otomatis saat Anda dalam perjalanan pulang dengan mengakses lokasi GPS Anda.

IoT kedengarannya keren tetapi masalahnya adalah bagaimana jika seorang *hacker* mengambil kendali atas peralatan rumah atau mobil Anda? Bagaimana jika peretas dapat meretas peralatan, perangkat, kendaraan atau seluruh bangunan pintar di internet? Hari ini ketika masyarakat memiliki informasi yang dicuri dari upaya peretasan, setidaknya mereka memiliki infrastruktur di tempat dan operasi dapat dipulihkan setelah data atau bagian manajemen krisis keamanan *cyber* berakhir. Tetapi dengan IoT, banyak hal dapat dengan cepat hilang jika seorang *hacker* dapat mengambil kendali atas peralatan yang dimiliki. Beberapa peralatan ini seperti perangkat medis yang terhubung juga dapat menyimpan data sensitif, yang dapat digunakan untuk melakukan kejahatan terkait identitas. Bahkan dalam hal

peralatan rumah tangga IoT, kekhawatiran timbul jika seseorang dapat mengendalikan kulkas pribadi yang terhubung kemudian merusak makanan dengan mengacaukan pendinginnya.

1. **Otentikasi berkelanjutan dengan Biometrik Perilaku**
   Biasanya kata sandi berfungsi sebagai penghalang antara pengguna dan informasi yang ia coba akses. Setelah penghalang ini dilewati, pengguna tidak pernah ditanya tentang otoritasnya sampai sesi terakhir. Pendekatan ini dapat memiliki hasil yang merusak jika seseorang yang tidak sah entah bagaimana dapat mengakses sistem TI dengan memberikan kata sandi yang ditebak atau menghindari keamanan. Otentikasi berkelanjutan adalah pendekatan di mana interaksi pengguna dengan sistem direkam dan profil dibuat darinya. Profil ini dihasilkan dari perilaku pengguna seperti cara mengetuk layar sentuh, dinamika *keypad*, data *accelerometer*, ukuran ujung jari, dll. Jika sistem otentikasi mendeteksi sesuatu yang tidak biasa selama sesi, ia dapat meminta pengguna untuk mengautentikasi ulang.

2. **Kontrol akses fisik ke sistem TI**
   Akses fisik ke ruang *server* atau pusat data dapat dimplementasikan dengan biometrik sehingga hanya individu yang berwenang yang dapat mendekatinya. Hal Ini juga mengurangi kemungkinan serangan orang dalam atau serangan fisik.

3. **Perangkat seluler yang diaktifkan secara biometrik untuk otentikasi biometrik**
   Sebagian besar pengguna yang mengerti teknologi membawa *smartphone* dengan satu atau lebih kemampuan

biometrik seperti sidik jari atau pengenalan wajah. Sistem otentikasi yang memanfaatkan kemampuan biometrik perangkat seluler akan menghilangkan kebutuhan keamanan berbasis kata sandi, tetapi juga akan memastikan bahwa perangkat diverifikasi dengan mengumpulkan data perangkat terlebih dahulu.

E. Penerapan Teknologi Biometrik Sidik Jari untuk Keamanan

Tahap-tahap dalam melakukan pra-pengolahan, pengolahan, dan identifikasi *object* adalah sebagai berikut :

1. *Membaca Citra*: Citra digital diperoleh dari foto mikroskopis kamera digital khusus *fingerprint* sehingga citra yang didapat sudah dalam bentuk file tanpa perlu dilakukan pemayaran (*scanning*) dengan format BMP.
2. *Cropping Citra*: Citra yang dipilih adalah citra 16-bit sehingga dikenali sebagai citra RGB. Untuk menyederhanakan proses perlu diubah intensitas warnanya menjadi keabuan, dimana citra hanya memiliki tingkat atau intensitas keabuan.
3. *Ekstraksi Area Citra*: Suatu objek dapat dengan mudah dideteksi pada suatu citra jika objek cukup kontras dari latar belakangnya. Perubahan kekontrasannya dapat dideteksi dengan deteksi tepi dengan menggunakan operator Sobel, yang menciptakan suatu citra biner. Untuk menentukan citra biner dengan menggunakan fungsi tepi.
4. *Deteksi Area Object*: Proses segmentasi dilakukan agar mendapatkan citra yang lebih baik, sehingga terlihat jelas objek- objek yang telah tersegmentasi, yaitu warna yang lebih kontras akan terlihat putih setelah dilakukan segmentasi. Pada citra asli, dapat terlihat celah pada garis yang mengelilingi objek pada gradien yang tersembunyi.

5. *Identifikasi Object*: Proses pengolahan citra digital berakhir dengan tampilan identifikasi citra hasil pengolahan. Karena program yang dibuat untuk mengidentifikasi sidik jari maka analisis yang diambil adalah mengidentifikasi dari database dibandingkan dengan hasil *scanning* langsung.

1. Pembacaan Citra yang Akan Diolah

Citra digital diperoleh dari foto mikroskopis kamera digital sidik jari yang sehat dan disimpan ke dalam database (sel sidik jari), sehingga citra yang didapat sudah dalam bentuk file tanpa perlu dilakukan pemayaran (*scanning*), dengan penyimpanan format jpg. Dalam program (Source-01) , pemilihan citra dilakukan dengan perintah:

```
% (Source-01)
clear all;close all;
a = imread ('nama file citra.format_citra');
imshow(a);
```

Gambar 5.3. Citra Asli Sidik Jari

2. Pengubahan Aras Warna Menjadi Aras Keabuan

Citra yang dipilih adalah citra 16-bit sehingga dikenali sebagai citra RGB. Untuk menyederhanakan proses perlu diubah aras warnanya menjadi aras keabuan, dimana citra hanya memiliki tingkat atau kadar keabuan. Program yang dibuat mengenali sel kanker prostat dalam aras keabuan. Dengan demikian citra dengan aras warna perlu diubah ke dalam aras keabuan. Hal ini dilakukan dengan perintah Matlab sebagai berikut.

% (Source-02)
b = rgb2gray (a);
imshow (b); title ('Aras Keabuan Citra');

Gambar 5.4. Citra asli sidik jari dan hasil Konversi keabuan

3. Proses Deteksi Tepi

Suatu objek dapat dengan mudah dideteksi pada suatu citra jika objek cukup kontras dari latar belakangnya. Perubahan kekontrasannya dapat dideteksi dengan deteksi tepi dengan menggunakan operator Sobel, canny, Robert, Otsu, LoG dan lainnya yang menciptakan suatu citra biner. Untuk menentukan citra biner dengan menggunakan fung-

si tepi. Hal ini dilakukan dengan perintah deteksi tepi sebagai berikut.

```
% (Source-03)
c = im2bw (b,'graythresh');
c = edge (c, 'sobel');
imshow (c); title (Citra dengan Deteksi Tepi);
```

Gambar 5.5. Citra Asli Sidik Jari dan hasil Deteksi Tepi

4. Segmentasi Citra

Proses segmentasi dilakukan agar mendapatkan citra yang lebih baik, sehingga terlihat jelas objekobjek yang telah tersegmentasi, yaitu warna yang lebih kontras akan terlihat putih setelah dilakukan segmentasi. Pada citra asli, dapat terlihat celah pada garis yang mengelilingi objek pada gradien yang tersembunyi. Hal ini dilakukan dengan perintah:

```
% (Source-04)
d  = imfill (c, 'holes');
d  = imclearborder (d, 8);
seD = strel ('diamond',1);
d  = imerode (d, seD);
d  = imerode (d, seD);
imshow(d);title('Segmentasi Citra');
```

5. Identifikasi Citra

Proses pengolahan citra digital berakhir dengan tampilan identifikasi citra hasil pengolahan. Karena program yang dibuat untuk mengidentifikasi sel sidik jari, maka analisis yang diambil adalah mengidentifikasi sel sidik jari yang ada dalam database dan sel sidik jari hasil scanning. Untuk mendapatkan selisih jumlah piksel antara citra acuan dan citra yang akan diolah, maka perlu ditampilkan citra *template atau citra acuan (dalam database). Dalam hal* ini yang digunakan sebagai citra acuan adalah citra sel sidik jari yang ada dalam database. Hal ini dilakukan dengan perintah sebagai berikut.

```
% (Source-05)
tmp = imread ('nama file citra.jpg');
tmp = rgb2gray(tmp);
tmp = im2bw(tmp,'graythresh');
tmp = edge(tmp,'sobel');
tmp = imfill (tmp, 'holes');
tmp = imclearborder (tmp, 8);
seD = strel ('diamond',1);
tmp = imerode (tmp, seD);
tmp = imerode (tmp, seD);
imshow(tmp);
```

Hasil dari citra acuan akan ditampilkan dengan perintah : ***imshow***

Dengan diketahuinya jumlah piksel maka dapat diperoleh dan ditampilkan kesimpulan mengenai jumlah piksel sel yang sehat dan dan jumlah piksel sel yang sakit dengan perbedaan banyaknya jumlah piksel. Proses untuk menghitung jumlah piksel putih untuk citra acuan dan citra yang akan diolah dilakukan dengan perintah:

```
Source-06.
% Hitung Jumlah Piksel Citra Acuan
[m,n,o]= size(tmp);
count  = 0;
for i = 1 : m;
  for j = 1 : n;
    if tmp(i,j) == 1;
       count = count + 1;
    else,
    end
  end
end
pix_ref = count;
% Hitung Jumlah Piksel Citra Yang Akan
Diolah
[m,n,o]= size(d);
count  = 0;
for i = 1 : m;
  for j = 1 : n;
    if d(i,j) == 1;
       count = count + 1;
    else,
    end
  end
end
pix_proc = count;
```

Perintah Source-06 akan dengan segera menghitung jumlah piksel putih, sehingga akan didapatkan jumlah piksel putih. Apabila jumlah piksel putih citra yang akan diolah lebih banyak dari jumlah piksel putih citra acuan, maka sel dikatakan tidak cocok, Jika jumlah piksel putih.

Apabila jumlah piksel putih citra yang akan diolah sama dengan jumlah piksel putih citra acuan, maka sidik jari cocok (teridentifikasi). Tabel 5.1. Menunjukkan hasil identifikasi 10 sidik jari dari 10 sidik jari di template yang disimpan dalam database dan hasil scanning secara langsung.

Tabel 5.1. Hasil Identifikasi 10 Sidik Jari dari Database dan dari *Scanning*

No. Sidik Jari	Jumlah Pixel sidik jari di database	Jumlah Pixel sidik jari hasil Scanning	Prosentase kemiripan	Hasil Identifikasi
1	1225	1346	91.01%	Cocok
2	1783	1952	91.34%	Cocok
3	778	778	100.00%	Cocok
4	797	927	65.98%	Tidak Cocok
5	914	1026	89.08%	Cocok
6	2427	2599	93.38%	Cocok
7	955	1071	60.17%	Tidak Cocok
8	1470	1617	90.91%	Cocok
9	1562	1697	92.04%	Cocok
10	1476	1476	100.00%	Cocok

Pembahasan hasil :

Tabel 5.1. adalah hasil identifikasi 10 sidik jari dari database dan dari sidik jari langsung dari *scanning*, di mana dapat diambil kesimpulan sebagai berikut:

a. Program (source 01 s.d 06) yang telah dibuat dapat mengidentifikasi sidik jari dalam database dibandingkan dengan hasil *scanning* dengan metode segmentasi dan menghitung jumlah piksel citra antara citra database dan citra hasil *scanning.*

b. Jumlah piksel minimum untuk citra sidik jari dalam database adalah 778 piksel, sedangkan jumlah piksel maksimumnya adalah 2427 piksel. Untuk citra sidik jari hasil scanning jumlah piksel minimumnya adalah 920 piksel dan jumlah piksel maksimumnya adalah 2599 piksel.
c. Prosentase hasil identifikasi sidik jari tingkat kemiripannya rata-rata: 92.30%, hasil penelitian ini menunjukkan tingkat akurasi sangat tinggi.
d. Hasil uji dari 10 citra sidik jari yang cocok 8 citra sidik jari dan 2 citra sidik jari yang tidak cocok, sehingga tingkat akurasinya 8/10x100% = 80%.

F. Penerapan Teknologi Biometrik Iris

Pada bagian ini akan dibahas mengenai hasil biometrik iris dengan pencitraan *multispectral* beserta hasil kecocokan *intra-spektral* dan *cross spectral*. Pengujian dilakukan pada 17 pasang mata dimana tiap mata diambil citra dengan 3 panjang gelombang yang berbeda dengan 10 pengambilan tiap panjang gelombang sehingga total terdapat 1020 citra iris. Pengambilan citra pada panjang gelombang 850 nm dilakukan dengan kondisi gain kamera 260 dan shutter ¼ sekon, untuk panjang gelombang 560 nm dilakukan dengan kondisi gain camera 1060 dengan shutter 1 sekon dan pada panjang gelombang 590 dilakukan dengan gain 260 dan shutter 1 sekon.

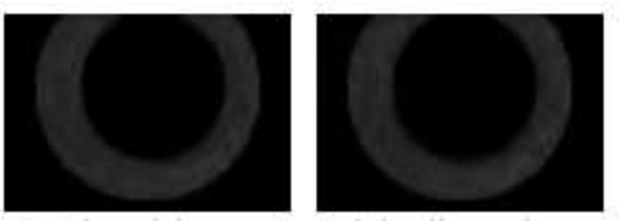
1. Deteksi Iris

Citra mata yang telah diperoleh kemudian diolah untuk mendapatkan citra iris, pengolahan dilakukan dengan algorithma daughman dimana pada setiap panjang gelombang yang berbeda, parameter jari-jari minimal pupil yang ada pada program pengolahan juga berbeda. Hal

ini dikarenakan pada panjang gelombang tampak, pupil mata akan bereaksi ketika ada cahaya yang masuk. Setiap pendeteksian iris memakan waktu paling lama 2,5 sekon. Dari 1020 citra iris , 880 berhasil dideteksi atau telah berhasil diperoleh keberhasilan pendeteksian sebesar 86%. 140 citra mata yang gagal untuk dideteksi irisnya diambil menggunakan panjang gelombang 850 nm. Kegagalan ini dikarenakan kurangnya fokus saat pengambilan data dan kegagalan program dalam mendeteksi lokal minima pada citra, lokal minima yaitu posisi paling gelap pada citra mata, yaitu pada pupil. Data yang diolah selanjutnya merupakan citra iris yang berhasil terdeteksi, Untuk citra yang memiliki noise seperti citra yang diambil pada panjang gelombang 590 nm dimana kondisi gain kamera 1060, maka dilakukan pra-prosesing seperti penghilangan noise dengan filter median.

2. Pencocokan Citra Iris

Sebelum dilakukan pencocokan maka ROI pada radius pupil dan iris tiap iris mata yang sudah terdeteksi disamakan, hal ini dilakukan untuk meningkatkan ketepatan perhitungan dikarenakan kondisi ukuran pupil yang berubah jika ada perubahan cahaya, selain itu bagian atas mata yang tertutup oleh kelopak mata atau alis dipotong.



Gambar 5.6. Citra iris yang sudah disamakan radius iris dan pupil

3. Distribusi Intra-Kelas

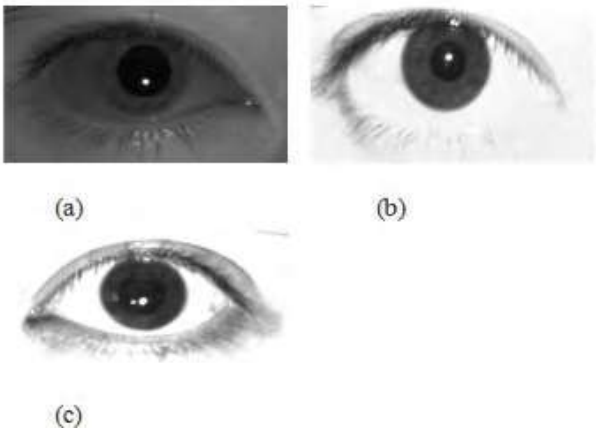
Nilai distribusi intra-kelas diperoleh ketika membandingkan citra sampel pada *spectral* yang sama dengan mata yang sama. Citra mata per panjang gelombang yang berjumlah 60 citra per pasang mata dibandingkan satu sama lain kemudian dijumlahkan dimana 4844 nilai intra-kelas ditampilkan pada gambar 4.4, 4.5 dan 4.6 di mana data rata-rata dan standar deviasi dari setiap hasil intra-kelas ditunjukkan pada tabel 4.1 di bawah ini.

Tabel 5.2 Rata-rata dan standar deviasi Intra-kelas

Panjang Gelombang	Rata-rata HD	Standar Deviasi HD
850 nm	0,25	0,087
590 nm	0,28	0,116
560 nm	0,29	0,122

Dapat dilihat pada hasil Gambar 4.5, 4.6 dan 4.7 intra-kelas pada panjang gelombang 590 dan 850 nm mempunyai standar deviasi dan rata-rata yang lebih kecil pada 560 nm, hal ini karena citra yang ditangkap pada pencahayaan 850 nm dan 590 nm tidak terdapat banyak motion blur dan noise, hal ini dikarenakan citra iris yang kurang terlihat pada penyinaran di panjang ge-

lombang ini sehingga gain kamera harus ditingkatkan hingga maksimum. Rata-rata tingkat kemiripan terendah didapat pada hasil citra iris dengan pencahayaan 560 nm, dapat dilihat pada gambar dibawah jika citra yang diambil pada panjang gelombang ini terlihat lebih gelap atau fitur pola iris kurang terlihat jika dibandingkan dengan citra yang diambil pada panjang gelombang diatasnya. Penyebab ketidak miripan pada keseluruhan spektral dikarenakan perubahan arah pandang, ketidakstabilan ukuran pupil dan perubahan jarak mata ke kamera.

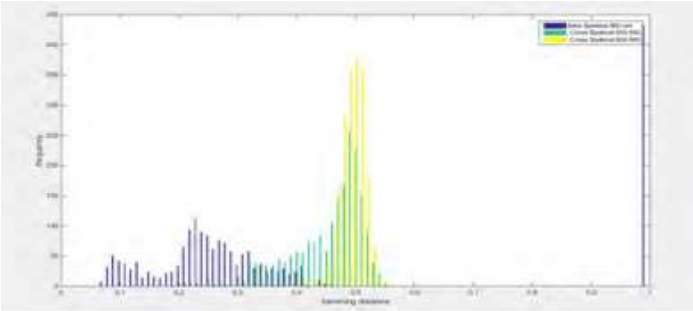


Gambar 5.7. Citra iris pada (a) 850 nm (b) 590 nm dan (c) 560 nm

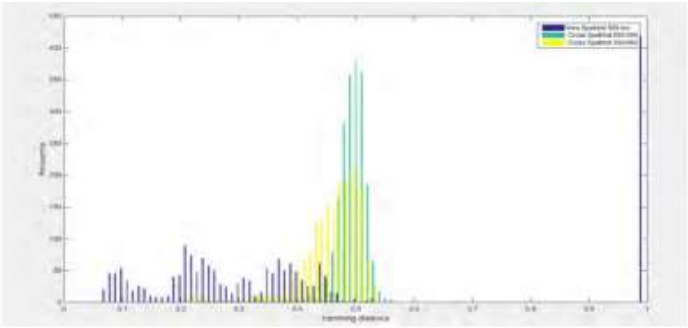
4. Distribusi Silang-Kelas

Nilai distribusi silang-kelas diperoleh ketika membandingkan citra sampel pada mata yang sama dengan spectral yang berbeda, hasil hamming distance dari pencocokan ini dijadikan tolak ukur kemiripan fitur iris yang ditangkap dengan sumber cahaya yang berbeda.

6000 nilai Silang-kelas iris pada tiap spectra tertentu akan dibandingkan masing-masing dengan spectra lainya. Grafik hasil pencocokan dapat dilihat pada gambar 4.5 – 4.7 di bawah ini.



Gambar 5.8. Grafik Silang-kelas panjang gelombang 850 nm dengan panjang gelombang lain



Gambar 5.9. Grafik Silang-kelas panjang gelombang 590 nm dengan panjang gelombang lain

False Rejection Rate (FRR): Presentase pengguna ditolak/dianggap sebagai penyusup. False Acception Rate (FAR): Presentase penyusup ditolak/dianggap sebagai

pengguna. *Equal Error Rate* (EER): Presentase di mana FAR dan FAR bertemu/memiliki nilai yang sama.

Tabel 5.3. FAR, FRR, ERR dan Akurasi pada silang-kelas 590 nm

Cross Spektral	FAR	FRR	EER	Akurasi
590-850	0,128	0,099	0,112	0,886
590-560	0,167	0,128	0,147	0,852

Tabel 5.4. FAR, FRR, ERR dan Akurasi pada silang-kelas 560 nm

Cross Spektral	FAR	FRR	EER	Akurasi
560-850	0,024	0,027	0,026	0,975
590-590	0,109	0,097	0,102	0,897

Tabel 5.5. Rata-rata dan Standar Deviasi Silang-Kelas

Panjang Gelombang	Rata-rata HD	Standar Deviasi HD
560-590 nm	0,54	0,064
580-560 nm	0,49	0,025
560-590 nm	0,53	0,055

Dari tabel 5.3 - 5.5 didapatkan hasil pengujian pembandingan fitur pada iris dengan panjang gelombang penyinaran 850, 590 dan 560 nm di mana akurasi terbaik didapatkan pada pasangan 850 dan 560 nm dengan mencapai 98% dan 97,5%, sedangkan untuk fitur pada iris dengan panjang gelombang penyinaran 590 nm mempunyai akurasi tertinggi 88,65%. Dari grafik Inter dan silang-kelas keseluruhan maka dapat diketahui bahwa pendeteksian iris dengan panjang gelombang 850 nm dan 560 nm mempunyai akurasi dan presisi

yang baik sehingga berpotensi untuk digunakan sebagai analisa biometrik gabungan untuk meningkatkan ketelitian pengidentifikasian iris maupun sebagai pendeteksi keaslian iris dikarenakan fitur iris dari hasil penyinaran 2 spektrum ini berbeda, dibuktikan dengan rata-rata nilai *hamming distance* silang-kelas pada kelas 850 nm dengan 560 nm sebesar 0,49.

06 Penerapan Teknologi Biometrik pada Bidang Medis

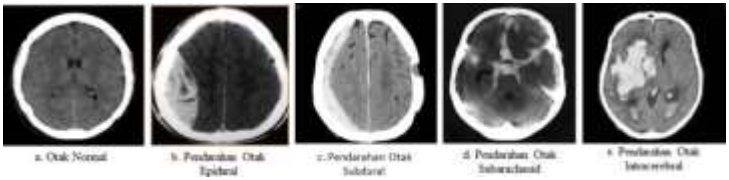
A. Pendarahan Otak Stroke

Otak adalah bagian organ tubuh yang sangat lunak dan lembut yang terdiri dari beberapa bagian. Bagian yang paling besar didominasi oleh serebrum, yang mengontrol kemampuan berbicara, ingatan, dan emosi. Otak sangat rawan mengalami kerusakan dan pendarahan. Pada prinsipnya otak mempunyai perlindungan yang sangat baik, karena otak telah dilindungi di berbagai lapisan. Di luar otak juga dilindungi oleh tengkorak beberapa jenis tulang yang saling berhubungan. Namun banyak faktor yang dapat menyebabkan pendarahan pada otak dan area sekitarnya. Pada pendarahan ada yang tidak bisa dikontrol pendarahan dapat menyebabkan kematian sel otak dan berhentinya banyak fungsi yang ada dalam tubuh dan yang bisa dikontrol.

Pada pendarahan yang tidak bisa dikontrol dapat menyebabkan matinya fungsi otak sementara atau permanen dan dapat mengakibatkan hilangnya kemampuan motorik. Terdapat 4 macam jenis pendarahan pada otak, yaitu (Graham, 1995). (1). Stroke dikategorikan menjadi sindroma klinis, untuk menentukan jenis stroke yang telah digambarkan menggunakan CT scan atau MRI (pencitraan) dapat dibedakan berdasarkan: vascular atau non-vascular (tumor atau infeksi) (2). Iskemik (stroke pendarahan), (3). infark arteri atau infark vena, (4). stroke sirkulasi anterior atau pesterior,

yang akan dipergunakan untuk menentukan apakah stenosis karotis bergejala atau tidak [13], seperti ditunjukan pada Gambar 1.

Teknologi pencintraan yang saat ini perkembangan sangat pesat seperti CT scan atau MRI dapat menggambarkan mana jaringan yang dapat diselamatkan pada pasien stroke sebelum mendapatkan perawatan dan pengobatan secara intensif. Namun CT scan atau MRI dapat menggambarkan pasien stroke apakah infark atau pendarahan memerlukan waktu 5 hari setelah akusisi pasien stroke. Untuk membedakan stroke pendarahan atau bukan stroke pendarahan biasa ditentukan berdasarkan intensitas tinggi atau putih, bentuknya bulat yang menenpel pada area infark biasanya intensitas rendah atau gelap yang menempati di beberapa area terjadi pembekakan seperti diperlihatkan pada Gambar 1.



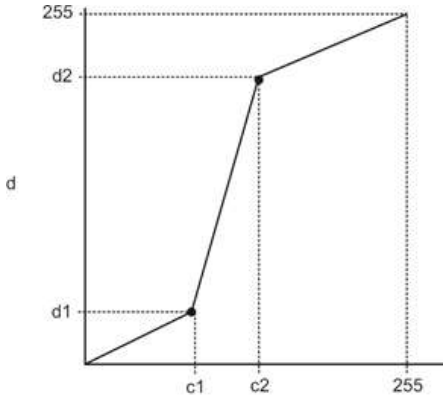
Gambar 6.1. Hasil CT Scan Otak Normal dan Pendarahan

Pada pasien indikasi stroke yang telah dilakukan akusisi menggunakan CT scan biasanya yang normal tidak mengalami pendarahan hal demikian oleh medis dianggap sebai infark. Jika dilakukan penajaman untuk interval kontras tidak diperlukan karena akan terjadi ketidak jelasan dari hasil diagnosis. Pendarahan kecil kadang tidak dapat terdikteksi berapa seharusnya intensitas tinggi (putih), sehingga menjadi tidak terlihat menjadi intensitas rendah dibandingkan dengan otak normal, ini meberikan informasi yang berbeda dari

infark atau bukan. Selama 10 hari, pendarahan kecil tidak akan bias membedakan antara infark dan perdarahan kecil, karena dalam 7 hari menghilang. Sedang Perdarahan besar tetap terlihat dalam waktu 2 sampa demgam 3 minggu. Optimasi diperlukan untuk mempercepat waktu dalam menggambarkan pasien stroke, CT scan atau MRI dapat menggambarkan citra pasien stroke untuk mendapatkan hasil diagnosis pasien apakah termasuk infark atau bukan infark. Karena hasil CT scan yang terindikasi infark tidak menjadi hipodensia butuk waktu berjam-jam bahkan bisa dalam 1 hari setelah terindikasi stroke [14].

B. Perentangan Kontras (*Contrast Stretching*)

SKontras dapat disebabkan oleh kondisi sinar yang tidak terdistribusi teratur pada bagian objek atau pengaruh keterbatasan jumlah sensor dalam merekam kejadian iluminasi. Gambar 2 menunjukan sebuah transformasi tipikal yang digunakan pada proses contrast stretching, dimana skala nilai antara 0 sampa dengan 255 dan diasumsikan bahwa citra memiliki skala keabuan.



Gambar 6.2. Hasil Transformasi Tipikal *Contrast Stretching*

Pada Gambar 6.2 digambarkan dua buah titik yaitu titik (c1,d1) dan titik (c2,d2) yang digunakan untuk menentukan pola sebagai fungsi transformasi, tujuan dari transformasi adalah untuk menentukan penyebaran intensitas skala keabuan pada citra yang diasumsikan. Jika c1=c2 dan d1=d2, maka terbentuk transformasi berupa garis lurus, maksudnya tidak terjadi perubahan intensitas keabuhan dari citra yang dihasilkan. Jika c1<=c2 dan d1<=d2, maka terbentuk transformasi dengan nilai tunggal dimana nilainya akan selalu naik.

C. Metode *Thresholding*

Thresholding atau operasi ambang batas adalah proses konversi input gambar kebuan ke gambar hitam putih menggunakan ambang optimal. *Thresholding* dapat bersifat lokal atau global (Naidu, dkk., 2017). *Thresholding* adalah sebuah metode segmentasi citra digital yang memfilter antara objek dan latarbelakang pada sebuah citra dibedakan atas tingkat kecerahan atau gelap intensitas citra. Region citra yang cenderung gelap akan bernilai intensitas 0), sedangkan region citra yang terang akan diberi nilai intensitas 1) [16]. Maka keluaran dari proses segmentasi dengan metode thresholding adalah berupa citra biner dengan nilai intensitas piksel sebesar 0 atau 1. Secara umum proses *thresholding* dapat dilakukan dengan persamaan (1).

$$g(X,Y) = \begin{cases} 1\ F(X,Y) < T \\ 0, f(x,y) \geq T \end{cases} \qquad (6.1)$$

1. Metode *Hybrid Thresholding*

Tujuan dari metode *hybrid image thresholding* adalah memanfaatkan karakteristik citra untuk membantu proses

penghitungan nilai *threshold.* Metode ini dikembangkan oleh Samopa [21] dengan tujuan untuk melakukan proses thresholding berdasarkan pada gabungan metode P-tile dan metode pendeteksian tepi. Sebagaimana dalam papernya berjudul *"Hybrid Image Thresholding Method Using Edge Detection",* Samopa menyatakan bahwa hasil segmentasi bentuk objek yang diperoleh lebih akurat dari metode biasa dan juga metode Otsu.

Memberikan nilai citra I menjadi citra aslinya dan G akan threshold batas nilai yang sedang mencari [17], algoritma *hybrid* metode *thresholding image* adalah sebagai berikut :

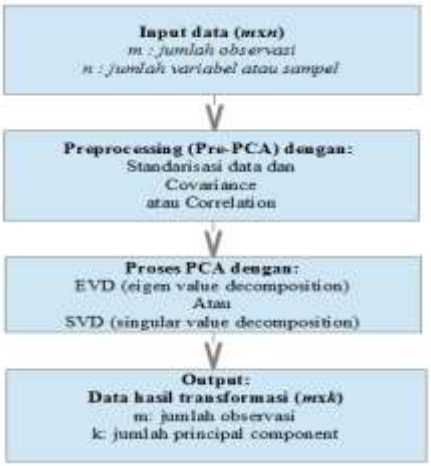
a. ←EdgeMap(I) # Hitung EdgeMap dari citra I #
b. v ← initial_Value
c. e ← RealMax # Set e sebagai nilai maksimum citra #
d. Loop until v = max_Value in Step increment.
e. T ← P-tile(I,v) # threshold I menggunakan P-tile metode dan v sebagai nilai threshold #
f. C ← EdgeMap(T) #Hitung Edge Mapdari citra T #
g. r ← MSE(O,C) # Hitung nilai MSE dalam O dan C #
h. If r < e # jika nilai MSE lebih kecil dari e #
i. e ← r # tukar nilai e dengan nilai MSE #
j. G ← v # set v sebagai nilai pencarian #

Metode ini sederhana dan cocok untuk semua jenis deteksi tepi, karena hanya iterasi dalam waktu terus-menerus (menentukan nilai langkah demi langkah). Metode ini tidak menambah lagi ke metode kompleksitas P-tile dan deteksi tepi membuat pendekatan *hybrid* ini. Dalam metode *hybrid image thresholding*, perlu menemukan tepi terbaik untuk digabungkan dengan deteksi tepi metode P -tile. Metode ini mencoba untuk menggabungkan metode P-tile dengan lima jenis deteksi tepi, canny, Pre-

witt, Roberts, Sobel dan Laplacian dari Gaussian (LOG) [17].

2. *Principal Component Analysis* (PCA)

PCA adalah teknik dalam menyederhanakan data menggunakan teknik proses transformasi linier, hasil transformasi terbentuk sistem koordinat baru dengan varians yang maksimal. Hasil proses PCA akan menghasilkan reduksi dimensi dari data dan tidak mengurangi kualitas dan karakteristik data secara senifikan [18]. Hasil penelitian Santosa tahun 2007 melakukan ekstraksi data yang banyak dan menghasilkan struktur data dengan pola yang baru dan sangat baik dan menghasilkan dimensi yang cukup banyak, di mana hasil ekstraksi telah menemukan eigen valu dan eigen vektor yang tepat dengan tingkat akurasi 98% [19]. Dalam proses transformasi tegak lurus dalam koordinat untuk mendiskripsikan data. Pemilihan koordinat harus menentukan variansi yang mencapai nilai maksimum. Gambar 3 menunjukkan cara kerja algoritma PCA, di mana PCA memproyeksikan citra dalam bidang ruang eigen-nya menggunakan teknik dengan mencari eigen vektor yang dimiliki setiap citra dan memproyeksikan dalam ruang eigen yang didapatkan. Nilai besaran dari ruang eigen ditentukan berdasarkan jumlah citra training yang digunakan [20]. Seperti dapat digambarkan pada gambar 3.

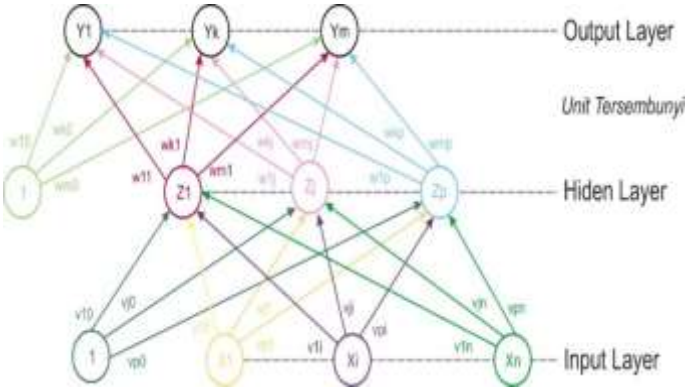


Gambar 6.3. Langkah-langkah Teknik PCA

3. *Backpropagation Neural Network*

Untuk mendapatkan keseimbangan kemampuan jaringan untuk mengenali pola yang digunakan untuk pelatihan diperlukan *backprogation neural network* yang disebut BNN, BNN digunakan untuk memberikan respon yang valid dari input pola yang mempunyai tingkat kemiripan (tetapi tidak sama) dengan pola yang digunakan selama pelatihan. BNN memiliki multi layer yang terdapat pada unit neuron yang tersembunyi. Arsitektur BNN dengan n buah input ditambah 1 bias dan m buah unit luaran (output). Arsitektur BNN dapat dilihat seperti pada gambar 4, dimana Vij sebagai bobot garis dari unit input Xi ke unit layer tersembunyi Zj (Vj0 adalah garis yang berhubungan dengan bias di unit input ke unit layer tersebunyi Zj). Sedangkan Wkj sebagai bobot dari unit layer tersebunti Zj ke unit luaran Yk (Wk0 sebagai bobot

dari bias layer tersebunyi ke unit luaran (Yk). Arsitektur BNN dapat digambarkan pada gambar 4.



Gambar 6.4. Arsitektur umum BNN dengan satu *hidden layer*

Penjelasan gambar 4 adalah sebagai berikut :

a. BNN dapat memiliki lebih dari 1 layer input dalam satu atau lebih layer tersebunyi. Arsitektur BNN dengan input ditambah dengan sebuah layer bias, sebuah layer tersembunyi terdiri dari p unit ditambah sebuah layer bias dan m buah unit luaran.
b. Vij sebagai bobot garis dari unit input Xi ke unit layer tersebunyi Zj, dimana Vj0 sebagai bobot garis yang menghubungkan layer bias pada unit input ke unit layer tersembunyi Zj. Wkj sebagai bobot dari unit layer tersebunyi Zj ke unit luaran Yk, dimana Wk0 sebagai bobot dari layer bias pada layer tersembunyi ke unit luaran Yk.

Algoritma Algoritma BNN dikenalkan pertama kali oleh Werbos dan dipopulerkan oleh Rumelhart dan Mc. Clelland. BNN adalah teknik perhitungan matematik

dengan rumusan yang menentukan setiap layernya. BNN merupakan jenis jaringan saraf tiruan (JST) dengan menggunakan metode pembelajaran terbimbing atau terawasi (*supervised learning*). Di mana pada *supervised learning* terdapat sepasang data input dan *output* yang digunakan untuk melatih jaringan saraf tiruan sampai didapatkan bobot penimbang (*weight*) yang diinginkan. Penimbang sebagai penghubung antarlayer dalam jaringan saraf tiruan. Algoritma BNN memiliki langkah proses pelatihan yang didasarkan pada interkoneksi (Penghubung) yang sederhana, yaitu Jika luaran masih memberikan hasil salah, maka penimbang dikoreksi agar nilai galat dapat diperkecil dan respon dari jaringan saraf tiruan selanjutnya diharapkan dapat mendekati nilai yang valid. Tahapan yang dilakukan pada algoritma BNN dijelaskan sebagai berikut :

a. Inisialisasi awal bobot dari nilai acak yang paling kecil antara 0 sampai dengan 1.
b. Setiap pasangan vektor dilakukan pelatihan mulai dari langkah 3 sampai dengan 8.
c. Setiap unit input (Xi dimana i=1,2,3...,n) menerima input Xi dan menjalankan input tersebut ke semua unit pada layer yang ada diatasnya atau selanjutnya sebagai hidden layer.
d. Setiap unit tersembunyi Zj, dimana j=1,2,3,..,p) jumlahkan bobotnya dengan nilai input masing-masing sengan persamaan :

$$Z_{netj} = v + \sum_{i=1}^{n}(xiyij) \qquad (6.2)$$

kemudian menggunakan fungsi aktivasi untuk menghitung nilai luarannya menggunakan persamaan :

$$Z = f(Z_{netj}) \qquad (6.3)$$

kemudian dikirimkan ke input tersebut ke semuan unit layer atasnya pada unit-unit luaran layer.

e. Setiap untuk luaran Yk, di mana k=1,2,3,..,m) jumlah bobotnya masing-masing menggunakan persamaan :

$$Y_{netk} = W_{ok} + \sum_{i=1}^{p}(ZiWk) \quad (6.4)$$

kemudian menggunakan fungsi aktivasi untuk menghitung nilai luarannya menggunakan persamaan :

$$y_k = f(Y_{netk}) \quad (6.5)$$

kemudian dikirimkan ke input tersebut ke semuan unit layer atasnya pada unit-unit luaran layer.

f. Setiap untuk luaran Yk, di mana k=1,2,3,..,m) menerima target pola yang terkoneksi dengan pola input pembelajaran, hitung informasi kesalahannya menggunakan persamaan :

$$\sigma_k = (t_k - y_k)\, f'(y_{netk}) = (t_k - y_k)\, y_k \quad (6.6)$$

Kemudian menghitung koreksi bobot yang akan digunakan untuk memperbaiki nilai Wjk, menggunakan persamaan :

$$\nabla W_{jk} = \sigma * \vartheta * Z_j \quad (6.7)$$

hitung juga koreksi bias yang akan digunakan untuk memperbaiki nilai W0k, kemudian dikirimkan ke unit-unit layer di bawahnya, menggunakan persamaan :

$$\nabla W_{jk} = \sigma \vartheta_k \quad (6.8)$$

g. Setiap unit tersembunyi Zj, di mana j=1,2,3,..,p) menjumlahkan delta inputnya dari unit-unit yang berada pada layer di atasnya, menggunakan persamaan:

$$\delta_{netj} = \sum_{k=1}^{m} (\delta_k W_{jk}) \quad (6.9)$$

kalikan nilai dengan turunan dari fungsi aktivasinya untuk menghitung informasi kesalahannya, menggunakan persamaan :

$$\delta_j = \delta_{netj} * f'(Z_{netj}) = \delta_{netj} Z_j (1 - Z_j) \quad (6.10)$$

kemudian hitung koreksi bobot yang akan digunakan untuk memperbaiki nilai Vij, menggunakan persamaan:

$$\nabla v_{jk} = \sigma * \delta_j X_i \quad (6.11)$$

hitung koreksi bias yang akan digunakan untuk memperbaiki nilai V0j, menggunakan persamaan:

$$\Delta v_{ok} = \sigma * \delta_j \quad (6.12)$$

h. Setiap unit luaran Yk, di mana k=1,2,3,..,m) untuk memperbaiki bias dan bobotnya, menggunakan persamaan:

$$W_{jk}(baru) = W_{jk}(lama) + \Delta v_{ok} \quad (6.13)$$

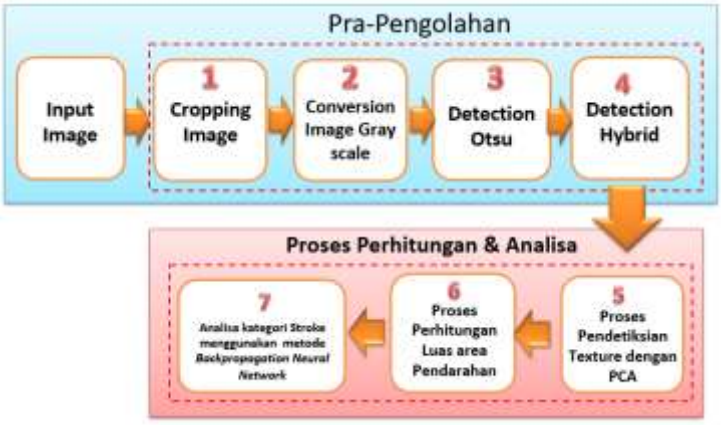
setiap unit tersembunyi Zj dimana j=1,2,3,..,p) memperbaiki bias dan bobotnya, dimana i=0,1,2,..,n), menggunakan persamaan :

$$v_{ij}(baru) = v_{ij}(lama) + \Delta v_{ij} \quad (6.14)$$

i. Pengujian kondisi berhenti.
Tahap 3 sampai dengan 5 merupakan bagian dari *feed forward,* tahap 6 sampai dengan 8 merupakan bagian dari *backprogation.*

D. Tahap-Tahap Pengujian

Dalam penelitian ini akan dilakukan analisis dan peningkatan kualitas citra pendarahan otak pasien stroke Epidural, Intra-cerebral, Subarachnoid, Subdural dari hasil CT-Scan dengan menggunakan metode *hybrid thresholding*. Tahapan penelitian yang akan dilakukan adalah sebagai berikut: studi literatur, perancangan sistem, pengujian dan evaluasi, publikasi ilmiah dan buku tesis. Tahapan-tahapan tersebut bisa dilihat pada Gambar 6.5.



Gambar 6.5. Tahap-tahap Pengujian

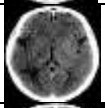
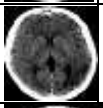
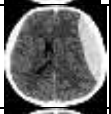
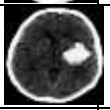
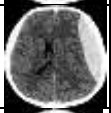
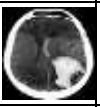
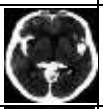
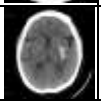
Uraian penjelasan tentang tahap-tahap dalam pengujian dapat dijelaskan sebagai berikut :

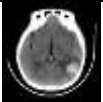
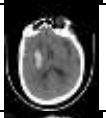
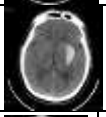
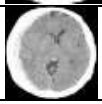
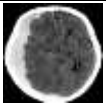
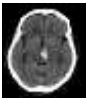
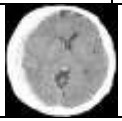
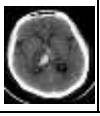
1. Citra input berasal dari CT scan / MRI yang diambil dari Rumah Sakit BMC Kota Padang akan disimpan dalam database menggunakan format jpg.
2. Citra berukuran 16-bit untuk dikenali sebagai RGB, untuk menyederhanakan proses maka perlu dilakukan perubahan intenstas dari RGB ke gray level, diperlukan algoritma untuk mengenali citra otak pendarahan dan yang normal.
3. Melakukan pemisahan antara objek dan latarbelakang, untuk dapat dideteksi dan ditentukan otak yang terjadi pendarahan, sehinga dapat dipisahkan antara pendarahan dan bukan pendarahan menggunakan metode Otsu.
4. Proses segmentasi dilakukan untuk mendapatkan pemisahan antara 1 atau lebih dari pendarahan agar dapat diketahui berapa jumlah pendarahan yang terjadi pada otak menggunakan metode hybrid thresholding.
5. Untuk mengidentifikasi pola pendarahan secara rinci agar dapat dianalisis maka ditentukan area pendarahan menggunakan metode PCA.
6. Melakukan perhitungan luas area pendarahan menggunakan algoritma hitung luas area pendarahan yang terdeteksi warna putih pada proses sebelumnya, sehingga didapatkan jumlah pixel intensitas putih area pendarahan otak.
7. Melakukan analisa dan klasifikasi pendarahan otak terkait dengan jenis stoke menggunakan metode BNN apakah termasuk stroke Epidural, Intracerebral, Subarachnoid, Subdural atau normal.

E. Hasil dan Analisa

Pengukuran volume pendarahan otak pasien stroke hemoragik intraserebral hasil MSCT, diawali dengan pengambilan data citra dari CT Scan, komputer *processing volume viewer*, menentukan target nilai volume pendarahan dari dokter spesialis radiologi 1 dan 2, dan hasil volume pendarahan dari hasil GVF snake. Hasil semua pasien pengukuran volume pendarahan dari computer Laboratorium Radiologi Rumah Sakit Bunda Medical Center (RS. BMC) Kota Padang dapat dilihat di Tabel 1.

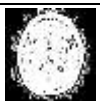
TABEL 6.1. Hasil semua pasien pengukuran volume pendarahan dari computer Laboratorium Radiologi Rumah Sakit Bunda Medical Center (RS. BMC) Kota Padang.

No.	Kode Pasien	Citra Asli	No.	Kategori stroke	Kode Pasien	Citra Asli	Kategori stroke
1.	P-01		16	Normal	P-16		Subarach noid
2.	P-02		17	Normal	P-17		Normal
3.	P-03		18	Epidural	P-18		Normal
4.	P-04		19	Epidural	P-19		Intracere bral
5.	P-05		20	Epidural	P-20		Subarach noid
6.	P-01		21	Intracere bral	P-21		Intracere bral

No.	Kode Pasien	Citra Asli	No.	Kategori stroke	Kode Pasien	Citra Asli	Kategori stroke
7.	**P-06**		22	Intracere bral	**P-22**		Epidural
8.	**P-07**		23	Subarach noid	**P-23**		Subdural
9.	**P-08**		24	Intracere bral	**P-24**		Intracere bral
10.	**P-10**		25	Subdural	**P-25**		Subarach noid
11.	**P-11**		*26*	Subdural	**P-26**		Epidural
12.	**P-12**		27	Subdural	**P-27**		Subarach noid
13.	**P-13**		28	Subdural	**P-28**		Epidural
14.	**P-14**		29	Subdural	**P-29**		Intracere bral
15.	**P-15**		30	Normal	**P-30**		Epidural

Hasil Peningkatan kualitas citra Pendarahan Otak dan Otak Normal hasil Deteksi Tepi dengan metode Hybrid Thresholding dapat dilihat di Tabel 2.

TABEL 6.2. Citra Pendarahan Otak dan Otak Normal Hasil Deteksi Tepi dengan Metode *Hybrid Thresholding*

Kd Pasien	*Hasil Streaching*	*Metode Hybrid Thresholding*	Kd Pasien	*Hasil Streaching*	*Metode Hybrid Thresholding*
P-01			P-16		
P-02			P-17		
P-03			P-18		
P-04			P-19		
P-05			P-20		
P-01			P-21		
P-06			P-22		
P-07			P-23		
P-08			P-24		
P-10			P-25		

Kd Pasien	*Hasil Streaching*	*Metode Hybrid Thresholding*	Kd Pasien	*Hasil Streaching*	*Metode Hybrid Thresholding*
P-11			P-26		
P-12			P-27		
P-13			P-28		
P-14			P-29		
P-15			P-30		

Proses Feature Extraction menggunakan PCA (***Principle Component Analysis)***

Pada langkah berikutnya adalah mengambil ciri pembeda dari bentuk atau bagian yang telah direpresentasikan sebelumnya dengan menggunakan metode PCA (*Principle Component Analysis*). Dataset Nilai piksel diambil dari salah satu citra sebagai berikut :

$$D= \begin{vmatrix} 0 & 0 & 0 & \dots & C_{10} \\ 0 & 128 & 128 & \dots & C_{20} \\ 0 & 0 & 255 & \dots & C_{30} \\ \dots & \dots & \dots & \dots & \dots \\ C_{91} & C_{92} & C_{93} & \dots & C_{100} \end{vmatrix}$$

Selanjutnya dilakukan *Zero Means* trhadap data di atas terlebih dahulu mencari vektor rata-rata dari dataset diatas setelah didapatkan matriks *Zero Means* dilakukan untuk perhitungan untuk mendapatkan matriks kovarian digunakan persamaan.

$$A = Y^T * Y$$

$$A = \begin{vmatrix} 0 & -85.3 & -85 \\ 0 & 42.7 & -85 \\ 0 & 42.7 & 170 \end{vmatrix} * \begin{vmatrix} 0 & 0 & 0 \\ -85.3 & 42.7 & 42.7 \\ -85 & -85 & 170 \end{vmatrix}$$

$$A = \begin{vmatrix} 14501.09 & 3582.69 & -18092.31 \\ 3582.59 & 9048.29 & -1262.71 \\ -18092.31 & -1262.71 & 30732.29 \end{vmatrix}$$

Kemudian dicari nilai eigen dari matriks kovarian diatas dengan persamaan 2.8 sebagai berikut :

$$[V, d] = eig(A)$$

eigen vektor

$$v = \begin{vmatrix} 592.051 & 355.198 & 517.933 \\ -66.130 & 474.322 & -144.332 \\ 412.475 & -16.851 & 439.493 \end{vmatrix}$$

eigen value

$$d = \begin{vmatrix} 0.017 & 0 & 0 \\ 0 & 4.571 & 0 \\ 0 & 0 & 59.432 \end{vmatrix}$$

Lalu hitung matriks *principal component analysis* dengan persamaan 2.10 sebagai berikut :

PCA = (Y * v)

-697.204	878.8453	-906.523	...	x_{10}
-883.438	-859.180	-818.151	...	x_{20}
767.531	-724.378	-693.507	...	x_{30}
...	...	...	...	x_{100}

TABEL 6.3. Citra Pendarahan Otak dan Otak Normal Hasil Perhitungan Area Pendarahan Dengan Algoritma Hybrid

Kd Pasien	*Metode Hybrid Thresholding*	*Luas Area dalam Pixel* (mm²)	*Kd Pasien*	*Metode Hybrid Thresholding*	*Luas Area dalam Pixel* (mm²)
P-01		**0.00**	**P-16**		**0.00**
P-02		**0.00**	**P-17**		**0.00**
P-03		2.530	**P-18**		1.764
P-04		2.336	**P-19**		3.037
P-05		3.085	**P-20**		2.101
P-01		3.001	**P-21**		6.911

Kd Pasien	*Metode Hybrid Thresholding*	*Luas Area dalam Pixel* (mm²)	*Kd Pasien*	*Metode Hybrid Thresholding*	*Luas Area dalam Pixel* (mm²)
P-06		1.594	**P-22**		5.810
P-07		3.033	**P-23**		5.629
P-08		3.369	**P-24**		5.840
P-10		3.791	**P-25**		6.839
P-11		9.102	**P-26**		8.268
P-12		2.606	**P-27**		6.339
P-13		2.661	**P-28**		1.845
P-14		3.	**P-29**		1.681
P-15		9.117	**P-30**		2.181

Klasifikasi menggunakan Metode *Bacpropagation Neural Network*

Tahap terakhir untuk mengklasifikasi pendarahan otak melalui citra hasil CT Scan adalah penggolongan ke dalam 5 jenis klasifikasi. Beberapa data diinput seebagai data latih, kemudian pengetahuan dan informasi yang diporeleh dari proses training tersebut digunakan sebagai acuan untuk klasifikasi pendarahan otak dengan menggunakan *Backpropagation Neural Network .*

Tahap Pengujian BNN menggunakan arah maju *(feed forward*), di mana fase ini data-data akan diuji adalah hasil dari ekstraksi fitur dan pola dan bukan merupakan data dari pelatihan. Bobot yang digunakan dalam pengujian ini adalah dari bobot hasil pelatihan, kemudian dilakukan perhitungan nilai keluaran di setiap node pada layer tersembunyi dan layer luaran. Setelah selesai pada tahap ini, kemudian dilakukan pengujian luaran untuk tiap-tiap node pada layer luaran. Jika hasil luaran node > 0.1, maka nilai luaran pada node akan diubah menjadi 0. Jika hasil luaran node < 0.1, maka nilai luaran pada node akan diubah menjadi 1. Dimana pada proses pengujian BNN data-data uji yang digunakan sebagai input adalah bobot dari hasil pelatihan.

Berikut hasil pengujian terhadap 30 pasien dan perhitungan luas area pendarahan otak menggunakan algoritma morphologi matematika dan hasil ekstraksi metode hybrid thresholding dapat dilihat di tabel 4.12. Terlihat bahwa dilakukan pengujian dari 30 pasien, yang terdiri dari 4 yang normal tidak terjadi pendarahan dan 4 Normal, 8 stroke Epidural, 7 stroke Intracerebral, 4 stroke Subarachnoid dan 7 stroke Subdural. Hasil pengujian yang dilakukan dihasilkan 4 Normal valid, 8 stroke Epidural terjadi 2 perbedaan yaitu pada P-30 dan P-04 seharusnya Epidural berubah P-30

menjadi stroke Subarachnoid dan P-04 menjadi stroke Intracerebral, 7 stroke Intracerebral semuanya valid, 4 stroke Subarachnoid valid dan 7 stroke Subdural terjadi perbedaan pada P-13 yang seharusnya stroke Subdural berubah menjadi stroke Subarachnoid. Seperti dapat dilihat pada tabel 4.

TABEL 6.4. Perbandingan Hasil Klasifikasi perhitungan dengan Alat DICOM dan Menggunakan Analisis *Hybrid Thresholding* (Otsu dan PCA) dan *Bagprogation Neural Network*

No	Kode Pasien	Luas Area Pendarahan Pixel (mm^2) dengan	Luas Area Pendarahan Pixel (mm^2) Dengan	Jenis Stoke	Hasil dengan Alat DICOM	Hasil klasifikasi Pengujian Sistem	Hasil pencocokan
1.	P-01	0.00	0.00	Normal	Normal	Normal	Valid
2.	P-02	0.00	0.00	Normal	Normal	Normal	Valid
3.	P-03	2.530	2.531	Sedang	Epidural	Epidural	Valid
4.	***P-04***	***2.336***	***4.336***	***Berat***	***Epidural***	***Intracerebral***	***Tidak Valid***
5.	P-05	3.085	3.085	Berat	Epidural	Epidural	Valid
6.	P-06	3.001	3.001	Berat	Intracerebral	Intracerebral	Valid
7.	P-07	1.594	1.594	Sedang	Intracerebral	Intracerebral	Valid
8.	P-08	3.033	3.033	Berat	Subdural	Subdural	Valid
9.	P-09	3.369	3.369	Berat	Intracerebral	Intracerebral	Valid
10.	P-10	3.791	3.791	Berat	Subdural	Subdural	Valid
11.	P-11	9.102	9.102	Berat	Subdural	Subdural	Valid
12.	P-12	2.606	2.606	Sedang	Subdural	Subdural	Valid
13.	***P-13***	***2.661***	***5.661***	***Berat***	***Subdural***	***Subbarachoi***	***Tidak Valid***
14.	P-14	3.001	3.001	Berat	Subdural	Subdural	Valid
15.	P-15	9.117	9.117	Berat	Subarachnoid	Subarachnoid	Valid
16.	P-16	0.00	0.00	Normal	Normal	Normal	Valid
17.	P-17	0.00	0.00	Normal	Normal	Normal	Valid
18.	P-18	1.764	1.764	Sedang	Intracerebral	Intracerebral	Valid
19.	P-19	3.037	3.037	Berat	Subarachnoid	Subarachnoid	Valid
20.	P-20	2.101	2.101	Sedang	Intracerebral	Intracerebral	Valid
21.	P-21	6.911	6.911	Berat	Epidural	Epidural	Valid
22.	P-22	5.810	5.810	Berat	Subdural	Subdural	Valid
23.	P-23	5.629	5.629	Berat	Intracerebral	Intracerebral	Valid
24.	P-24	5.840	5.840	Berat	Subarachnoid	Subarachnoid	Valid
25.	P-25	6.839	6.839	Berat	Epidural	Epidural	Valid
26.	P-26	8.268	8.268	Berat	Subarachnoid	Subarachnoid	Valid
27.	P-27	6.339	6.339	Berat	Epidural	Epidural	Valid
28.	P-28	1.845	1.845	Ringan	Intracerebral	Intracerebral	Valid
29.	P-29	1.681	1.681	Ringan	Epidural	Epidural	Valid
30.	***P-30***	***2.181***	***1.181***	***Ringan***	***Epidural***	***Subbarachoi***	***Tidak Valid***

Berdasarkan data hasil uji yang telah dilakukan pada aplikasi klasifikasi pendarahan otak melalui citra CT Scan menggunakan analisis *Hybrid Thresholding* (Otsu dan PCA) dan *Backpropagation Neural Network*, dapat diperoleh nilai akurasi dalam pengidentifikasian luas area pendarahan otak dan klasifikasi stroke. Dari perhitungan luas area pendarahan dapat diketahui bahwa tingkat akurasi dari metode yang digunakan dalam menganalisis pendarahan otak dalam mengklasifikasikan stoke dengan citra CT Scan yaitu 27 / 3 x 100% = 90.0%. Kesalahan klasifikasi terjadi karena kemiripan fitur hasil dari analisis segmentasi dan ekstraksi menggunakan *Hybrid Thresholding* dan klasifikasi dengan Backpropagation *Neural Network*. Pada penelitian ini, kesalahan tersebut terdapat pada klasifikasi pasien dengan kode pasien P-04 dari stroke epidural menjadi intracerebral, P-13 dari subdural ke subbarachoid, dan P-24 dari epidural ke subbarachoid. Hasil perhitungan jumlah piksel yang putih setelah dilakukan segmentasi *hybrid thresholding* dan ekstraksi fitur menggunakan PCA terjadi kesamaan.

DAFTAR PUSTAKA

A. Aglio-Caballero, B. Rios-Sanchez, C. Sanchez-Avila, and M. J. M. De Giles. 2017. Analysis of local binary patterns and uniform local binary patterns for palm vein biometric recognitione, vol. 2017-Octob, pp. 1–6.

A. Ross, K. Nandakumar, and A. Jain, *Handbook of multibiometrics*, vol. 6. 2006.

A. Ross, R. Pasula, and L. Hornak. 2009. Exploring multispectral iris recognition beyond 900nm. *IEEE 3rd Int. Conf. Biometrics Theory, Appl. Syst. BTAS*.

A. Y. Rahman and S. Sumpeno. 2016. Segmentasi Arca pada Museum Mpu Tantular Sidoarjo Menggunakan Learning Vektor Quantization, no. December, pp. 16–21,

A. Y. Rahman, S. Sumpeno, and M. H. Purnomo, "*Video minor stroke extraction using learning vektor quantization*," 2017 5th Int. Conf. Inf. Commun. Technol. ICoIC7 2017, no. July 2018, 2017.

Ahmadjayadi, Cahyana. 2004. *Konsep Pengamanan dan Perlindungan Infrastruktur Berbasis teknologi Informasi*, Kementrian Komunikasi dan Informasi, Information System Security Control and Audit Conference 2004.

Apley, A. Graham. 1995. Dalam: *Buku Ajar Orthopedi dan Fraktur Sistem Apley*. Ed. Edi Nugroho Widya Medica, Jakarta.

Attaway, S. 2017. *Matlab A Practical Introduction to Programming and Problem Solving* (4th ed.).

Ax-S Biometric. 2005. *Biometric Security Risk Assessment*. Available: <http://www.ax-sbiometrics.com/Downloads/ PhysicalRiskAssessmentbrief.pdf>

Byrne, Jim. 2003. Large-Scale Biometric Management: A-Centralized, Policy-based Approach to Reducing Organizational Identity Chaos. *Information System Control Journal*, Vol 6, page 41-44.

C. Ching Ho, M. Ali Hussin, and H. Ng. 2015. Match score fusion of fingerprint and face biometrics for verification, vol. 77, no. 18, pp. 93–102.

C. Leiva-Salinas, B. Jiang, and M. Wintermark. 2018. Computed tomography, computed tomography angiography, and perfusion computed tomography evaluation of acute ischemic stroke. *Neuroimaging Clinics of North America,* vol. 28, no. 4, pp. 565–572.

C. Whitelam, Z. Jafri, and T. Bourlai. 2010. Multispectral eye detection: a preliminary study. *Proc.-Int. Conf. Pattern Recognit.*, pp. 209–212.

Canadian Stroke Strategy. 2010. *Canadian best practice recommendations for stroke care update 2010*. Canada.

Chandra, Akhilesh & Calderon, Thomas G. 2003. Toward a Biometric Security Layer in Accounting Systems. *Journal of Information Systems*, page 51-70.

D. Setiawan, I. Arifin, and R. Ardianto. 2018. Implementasi Pengembangan Sistem Media Pembelajaran Pengenalan Komputer: Program Studi Sistem Informasi Universitas PGRI Madiun*. Intensif*, vol. 2, no. 2, pp. 127–135,

Donny, *Cracker.* 2005. *Sebab Akibat dan Kepastian Hukum, Information and Communication Technology Watc*h,

Available: <http://free.vlsm.org/v17/com/ictwatch/paper/paper061. htm>

E. Mosley and D. Irvine. 2019. *How Recognition Works*.

F. Hlawatschg and F. Auger. 2008. *Time-Frecuency Analysis*.

F. Ilmu, U. Sains, J. Raya, and S. Padang. 2018. Sistem informasi pembelajaran identifikasi dan pengenalan dini bahasa suku sentani berbasis kearifan lokal. vol. 2, no. 12, pp. 9–16,

Gilat, A. 2017. *MATLAB An Introduction with Applications.* Wiley (6th ed.). Wiley.

Gökberk, B., Salah, A. A., & Akarun, L. 2005. Rank-based decision fusion for 3D shape-based face recognition. In *International Conference on Audio-and Video-Based Biometric Person Authentication* (pp. 1019-1028). Springer, Berlin, Heidelberg.

Gong, S., Liu, C., Ji, Y., Zhong, B., Li, Y., & Dong, H. 2019. Advanced Image and Video Processing Using MATLAB. *Springer* (Vol. 12). https://doi.org/10.1007/978-3-319-77223-3

Gonzalez, R. C., & Woods, R. E. 2008. *Digital Image Processing*. Prentice Hall.

Hanselman, D., & Littlefield, B. 2012. *Mastering MATLAB*. Pearson. Pearson.

International Biometric Group, Available: <http://www.biometricgroup.com/reports/public/ market_report.html> (2005, 17 Januari). "*Biometric Market and Industry Report 2004-2008*".

J. Daugman and C. Downing. 2001. Epigenetic randomness, complexity and singularity of human iris patterns. *Proc. Biol. Sci.,* vol. 268, no. 1477, pp. 1737–40.

J. Daugman. 2007. New methods in iris recognition. *IEEE Trans. Syst. Man. Cybern. B. Cybern.,* vol. 37, no. 5, pp. 1167–1175.

J. Gomes and L. Velho. 1999. From Fourier Analysis to Wavelets. *ACM SIGGRAPH '99 Courses -SIGGRAPH '99*, pp. 1–210.

J. M. Medina, L. M. Pereira, H. T. Correia, and S. M. C. Nascimento. 2011. Hyperspectral optical imaging of human iris in vivo: characteristics of reflectance spectra. *J. Biomed. Opt.*, vol. 16, no. 7, p. 076001.

Jastal, Udin Y, Veridiana N, dkk. 2020. *Riset kesehatan dasar dalam angka Provinsi Sulawesi Tengah 2020*. Badan Penelitian dan Pengembangan Kesehatan Kementerian Kesehatan RI, Sulawesi Tengah.

Jawa Pos (2005, 5 Januari) "*Tas Berteknologi Biometric*", Available: <http://cdc.eng.ui.ac.id> Liu, Simon & Silverman, Mark, "A Practical Guide to Biometric Security Technology", Computer Society, Available: <http:\\www.computer.org> (2005, 5 Januari).

Kadir, A., Nugroho, L. E., Susanto, A., & Santosa, P. I. 2012. Performance improvement of leaf identification system using principal component analysis. *International Journal of Advanced Science and Technology*, 44(11), 113-124.

Kim AS, and Jhonston SC. 2011. Global variation in the relative burden of stroke and ischemic heart disease. *Circulation*; 124:314-323.

L. Shen and L. Bai. 2006. A review on Gabor wavelets for face recognition. *Pattern Anal. Appl*., vol. 9, no. 2–3, pp. 273–292.

M. A. Kalafut, D. L. Schriger, J. L. Saver, and S. Starkman. 2000. *Detection of early CT signs of >1/3 middle cerebral artery infarctions: interrater reliability and sensitivity of CT interpretation by physicians involved in acute stroke care*. *Stroke,* vol. 31, no. 7, pp. 1667–1671.

M. J. Burge and K. Bowyer. 2013. *Handbook of Iris Recognition.*

M. Misiti, Y. Misiti, G. Oppenheim, and J.-M. Poggi. 2020. *Wavelet Toolbox Computation Visualization Programming User‟s Guide*.

M. N. Osman, K. A. Sedek, M. Maghribi, and N. Hidayah. 2018. ANotify : A Fingerprint Biometric-Based and Attendance Web-Based Management System with SMS Notification for Industrial Sector. vol. 3, no. 1, pp. 36–45.

M. Stanuch and A. Skalski. 2018. Artificial database expansion based on hand position variability for palm vein biometric system*. IST 2018-IEEE Int. Conf. Imaging Syst. Tech. Proc.*, pp. 1–6.

Media Indonesia (04 Juli 2002), "*Survei Terhadap 450 CIO-Perencanaan Keamanan Sistem Informasi Lemah*.", Nakertransnet, Available: <http://www.nakertrans.go.id> (2005, 4 Januari).

O. Percy. *Iris localization using Daugman ‟ s algorithm*, pp. 1–48.

P. Meredith, B. J. Powell, J. Riesz, S. P. Nighswanderrempel, R. Pederson, And E.G. Moore. 2006. *Towards structure–property–function relationships for eumelanin*, pp.37–44.

Panella M, Marchisio S, Brambilla R, *et al*. 2012. A cluster randomized trial to assess the effect of clinical pathways for patients with stroke: results of the clinical pathways for effective and appropriate care study. *BMC Medicine*;10 (71).

Perdana, Arizky. 2010. Studi Pengguna Komputer Bicara dalam Menyelesaikan Tugas Akademik Mahasiswa Tunanetra di PLB UNESA. *Skripsi tidak diterbitkan*: PLB FIP UNESA.

Prameswary, Ruth Novita. 2008. *Persepsi Pengguna Mengenai Software Jaws Screen Reader*: Studi Kasus di Yayasan Mitra Netra (online), (http:// lontar. ui.ac.id/, diakses pada 10 Desember 2012).

Presiden Republik Indonesia. 2004. *Undang-Undang Republik Indonesia Nomor 20 Tahun 2003* Tentang Sistem Pendidikan Nasional. Jakarta: Departemen Pendidikan Nasional.

Purwanto, Eka. 2006 . Relevansi Komputer Bicara Terhadap Kebutuhan Tunane. *Jurnal Pendidikan Luar Biasa* April 2006, Volume 2, Nomor 1. Surabaya: Uni Press Unesa.

Qiu W, Kuang H, Teleg E, Ospel JM, Sohn SI, Almekhlafi M, Goyal M, Hill MD, Demchuk AM, Menon BK. 2020. Machine Learning for Detecting Early Infarction in Acute Stroke with Non-Contrast-enhanced CT. *Radiology*, 294(3) 638-644. doi:10.1148/radiol.2020191193. PMID: 31990267.

R. Chen, X. Lin, and T. Ding. 2012. Liveness detection for iris recognition using multispectral images. *Pattern Recognit. Lett.,* vol. 33, no. 12, pp. 1513–1519.

R. Polikar. 1994. *the Wavelet Tutorial Second Edition Part I* By," Internet Resour. httpengineering rowan edu polikarWAVELETSWTtutorial html, pp. 1–67, 46.

Radio Singapore International (19 Oktober 2004). "*Lebih Aman Dengan Paspor Biometrik*", <http://www.rsi.com. sg>(di akses : 4 Januari 2021).

Roger V, Go A, Lloyd-Jones D, *et, al*. 2011. *Heart disease and stroke statistics 2011* update: A report from the American Heart Association. Circulation;123:18-209.

Romney, Marshall B and Steinbart, Paul John. 2003. *Accounting Information Systems*, Ninth Edition, Prentice Hall.

Ross, Steven J. 2003. *Who Needs Information Security*. *Information System Control Journal*, Vol 6, page 9-10.

S. Emerich and B. Belean. 2018 Biometrics Recognition based on Image Local Features Ordinal Encoding. *Int. J. Adv. Comput. Sci. Appl*., vol. 8, no. 12.

S. Minhas and M. Javed Younus. 2009. Iris Feature Extraction Using Gabor Filter. *Comput. Eng*., pp. 252–255,

S. W. P. Marios Savvides, Jingu Heo. 2008. *Handbook of Biometrics*.

Samopa, F., & Asano, A. 2009. Hybrid image thresholding method using edge detection. *International Journal of Computer Science and Network Security*, 9(4), 292-299.

Smith, L. I. 2002. *A tutorial on principal components analysis.*

SP18 (2005, 4 Januari). *IBM Gunakan Pengaman Biometric Untuk Notebook*, Available: http://www.sp18. com.

Sumijan, AW Purnama, S Arlis. 2019. Peningkatan Kualitas Citra CT-Scan dengan Penggabungan Metode Filter Gaussian dan Filter Median. *Jurnal Teknologi Informasi dan Ilmu Komputer,* 2019, (Vol. 6. No. 6, p-ISSN: 2355-7699, e-ISSN: 2528-6579).

Sumijan, M.S., Harlan, J. and Wibowo, E.P., 2017. Hybrids Otsu method, feature region and mathematical morphology for calculating volume hemorrhage brain on CT-scan image and 3D reconstruction. *TELKOMNIKA Telecommunication, Computing, Electronics and Control,* 15(1), pp.283-291.

Sumijan, Purnama, P.A.W. and Arlis, S. 2019. Multiple Thresholding Methods for Extracting & Measuring Human Brain and 3D Reconstruction. *In Journal of Physics: Conference Series,* Vol. 1339, No. 1, p. 012027. IOP Publishing.

Sutoyo, T. D., Mulyanto, E., Suhartono, V., & Nurhayati, O. D. 2009. *Teori pengolahan citra digital*. Yogyakarta: Andi.

T. Moloharto, S. Al Faraby, and K. M. Lhaksmana. 2019. Implementasi Alignment Point Pattern Pada Sistem Pengenalan Sidik Jari Menggunakan Sidik Jari Menggunakan Template Matching. *e-Proceeding Eng*., vol. 6, no. 1, pp. 2442–2450.

T. S. Lee. 2002. Image representation using 2d gabor wavelets. *IEEE Trans. Pattern Anal. Mach. Intell*., vol. 18, no. 10, pp. 959–971, 1996. [13] L. Ma and Y. Wang. Iris recognition based on multichannel Gabor filtering. *Proc. Fifth Asian Conf. Comput.,* no. 59825105, pp. 1–5,

Tentu, A. N., Basit, A., Bhavani, K., & Venkaiah, V. C. 2017. *Multi-secret sharing scheme for level-ordered access structures. In International Conference on Number-*

Theoretic Methods in Cryptology (pp. 267-278). Springer, Cham.

Tongia, Rahul and Jain, Kanika. 2003. Investing in Security-Do Not Rely on FUD. *Information System Control Journal*, Vol 6, page 27-28.

U. Vovk, F. Pernuš, and B. Likar. 2007. A review of methods for correction of intensity inhomogeneity in MRI. *IEEE Transactions on Medical Imaging*, vol. 26, no. 3, pp. 405–421.

Uchino K, Pary J, Grotta J. 2011. *Acute Stroke Care*, 2nd ed, New York: Cambridge University Press.

Wallhoff, John. 2003. *Enforce Security with a Fingerprint Biometric Solution*. *Information System Control Journal*, Vol 4, page 39-43.

Warren, Carl, S., Reeve, James, M. dan Fess, Philip, E. 2005. *Accounting, 21th edition*. Thomson Learning.

Weber, Ron. 1999. Information Systems Control and Audit, Prentice Hall.

WHO. 1997. Stroke trends in the WHO MONICA project. *Stroke;* 28:500-506.

Y. Zhang, M. Brady, and S. Smith. 2001. Segmentation of brain MR images through a hidden Markov random field model and the expectation-maximization algorithm. *IEEE Transactions on Medical Imaging*, vol. 20, no. 1, pp. 45–57.

TENTANG PENULIS

Sumijan, dilahirkan di Nganjuk pada tanggal 7 Mei 1966 dari Bapak Pardi (Alm) dan Ibu Saikem, anak ke enam dari 7 bersaudara. Menikah dengan Yetri Desmiyanti dan dikaruniai 4 orang anak yaitu : 1. Pradani Ayu Widya Purnama, S.Kom., M.Kom. (Tempat/ Tanggal Lahir : Padang / 8 Maret 1993), 2. Ratu Mas Ayu Atika Putri Ramadhanty, S.Pd., M.Pdt. (Tempat/ Tanggal Lahir: Padang/8 Maret 1994), 3. Danny Andika Putra, S.E., M.M. (Tempat/Tanggal Lahir: Padang / 8 Desember 1995), 4. Putri Ayu Debie Mustika Sari (Tempat/Tanggal Lahir: Padang / 24 Desember 2003).

Riwayat Pendidikan: Program *Sarjana* (S1) Jurusan Manajemen Informatika Sekolah Tinggi Manajemen Informatika (STMIK) YPTK Padang, Program *Magister* (M.Sc) dari University Teknologi Malaysia (UTM) Malaysia, Program *Doktor* (Ph.D) dari Universitas Gunadarma Jakarta. Bidang keahlian : *Medical Image Processing, Sistem Pakar, dan Data Mining.*

Saat ini bertempat tinggal di Komp. Palm Griya Indah No. 1 Marapalam Indah, Kec. Lubuk Begalung, Padang, Sumatera Barat, email : soe@upiyptk.org, HP. 08126607355, situs: http://upiyptk.ac.id/soe/http://sisfo.upiyptk.ac.id.

Pradani Ayu Widya Purnama, S.Kom., M.Kom. adalah dosen tetap Fakultas Ilmu Komputer, Universitas Putra Indonesia "YPTK" Padang sejak 2016. Pendidikan Sarjana (S1) di Kampus Universitas Putra Indonesia "YPTK" Padang Tamat 2014, bidang Teknik Informatika. Maraih Gelar Master dalam bidang Information Technology di Universitas Putra Indonesia "YPTK" Padang ditamatkan tahun 2016, bidang keahlian: *Data Mining dan Artificial Intellegence.*

Syafri Arlis, S.Kom., M.Kom. adalah dosen tetap Fakultas Ilmu Komputer, Universitas Putra Indonesia "YPTK" Padang sejak 2010. Pendidikan Sarjana (S1) di Universitas Putra Indonesia "YPTK" Padang Tamat 2009, bidang Sistem Informasi. Maraih Gelar Master dalam bidang Teknologi Informasi di Universitas Putra Indonesia "YPTK" Padang pada tahun 2011. Sekarang sedang menempuh pendidikan Program Doktor Teknologi Informasi, Fakultas Ilmu Komputer, Universitas Putra Indonesia "YPTK" Padang sejak 2019 dan sekarang sedang menyelesaikan disertasi. Bidang keahlian: *Digital Image Processing dan Database.*