

## Sistem Otentifikasi Sidik Jari menggunakan Metode Minutiae Matching berbasis *Average Euclidean Distance*

Hendri Himawan Triharminto<sup>1</sup>, Almira Budiyanto<sup>2</sup>

<sup>1</sup> Jurusan Teknik Elektro Pertahanan, Akademi Angkatan Udara

<sup>2</sup> Jurusan Teknik Elektro, Universitas Islam Indonesia

Korespondensi : [kanghimawan@gmail.com](mailto:kanghimawan@gmail.com)

### ABSTRAK

Sistem biometrik berbasis sidik jari menjadi salah satu pengamanan standar yang dikembangkan di perkantoran-perkantoran serta untuk memeriksa kehadiran para pekerja yang hadir di kantor. Metode yang biasa digunakan dalam melakukan pendeteksian sidik jari adalah dengan mengekstraksi citra yang dihasilkan dari sensor sidik jari. Ekstraksi citra tersebut akan menghasilkan ciri khusus yaitu minutiae. Dengan kekhasan masing-masing orang berkaitan dengan minutiae, maka hal tersebut dapat dijadikan basis dalam melakukan deteksi sidik jari. Langkah awal metode yang digunakan dalam otentifikasi sidik jari adalah dengan mengubah citra menjadi biner agar dapat diterapkan metode *thinning image*. Setelah *thinning image* diterapkan, maka ekstraksi minutiae dapat dilakukan dengan mengidentifikasi ridge bifurcation dan ridge ending pada citra. Penelitian ini hanya menggunakan dua jenis minutiae. Langkah selanjutnya dalam fitur ekstraksi adalah *matching* citra untuk menguji kemiripan antara data pengujian dan database. *Euclidean distance* digunakan untuk menguji kemiripan antar citra, dimana *thresholding method* digunakan untuk menentukan tingkat kemiripan. Penelitian ini menambahkan perumusan rata-rata *Euclidean distance* dengan mempertimbangkan seluruh nilai database pada sidik jari orang yang sama. Untuk menguji hasil dari penambahan metode tersebut, maka digunakan data set standar internasional DB1 dengan 10 jenis sidik jari dari orang yang berbeda. Dari hasil pengujian yang dilaksanakan, dapat dilihat bahwa metode yang diterapkan mempunyai akurasi 81.25% sehingga dapat digunakan sebagai salah satu metode dalam memecahkan masalah identifikasi sidik jari.

Kata kunci: Sidik jari, minutiae, *matching*

### ABSTRACT

*The fingerprint-based biometric system is one of the safety standard in office and used to check employee attendance. The method that commonly used in fingerprints detection, is image extraction from fingerprint sensor acquisition. The image extraction will produce a special feature which is called minutiae. Each person has a specific minutiae that can be used as a basis for fingerprint detection. First step regarding to fingerprint detection is to convert the image into binary thus thinning image method can be implemented to obtain skeleton image. After image thinning is applied, extraction minutiae is following by ridge bifurcation and ridge ending identification on the image. This research merely uses two types of minutiae. The next step in the extraction feature is image matching to test the similarity between the image from the data test and database. Euclidean distance is used to test the similarity both of images and thresholding method is to determine the degree of similarity. This study enhances the method by adding average Euclidean distance formulation, which considers the value from all similar fingerprints database. In order to test the result of the proposed method, the DB1 international standard data set are used which consist of 80 types of fingerprints from 10 different people. The result shows that the method applied has an accuracy of 81.25% which means that the method can be used as an algorithm to solve fingerprint detection problem..*

*Keyword : Fingerprint, minutiae, matching*

### 1. PENDAHULUAN

Otentifikasi adalah suatu hal yang penting agar tidak semua orang dapat mengakses area-area atau ruangan-ruangan yang rahasia. Dalam dunia militer tentunya otentifikasi menjadi bagian dari pengamanan terhadap area terbatas yang hanya diperbolehkan bagi orang-orang yang berkepentingan. Ruangan-ruangan yang menyimpan data rahasia haruslah disertai dengan pengamanan yang hanya dapat dibuka dengan sistem otentifikasi. Salah satu otentifikasi yang saat ini sedang berkembang dan telah menjadi pengamanan standar adalah yang otentifikasi berbasis biometrik.

Sistem biometric menggunakan perilaku dan fisiologi sebagai sarana untuk melakukan otentifikasi. Tanda tangan dan mengisi password adalah contoh dari sistem biometrik yang menggunakan perilaku. Kelemahan dari sistem biometric yang berbasis perilaku adalah konsistensi dan dapat berubah berdasarkan

waktu. Disisi lain, biometrik berdasarkan karakter fisiologi seperti wajah, sidik jari, telapak tangan dan iris tetap tidak berubah sepanjang waktu hidup seseorang dan tidak mudah untuk dipalsukan sehingga dari mempunyai keamanan yang cukup tinggi [1]. Berkaitan dengan hardware yang dikembangkan, sidik jari menjadi standar keamanan di perkantoran-perkantoran dan dijadikan salah satu fasilitas untuk mengetahui kehadiran seseorang saat bekerja karena memberikan hasil yang lebih akurat dari mayoritas sistem biometrik yang lain dan tidak memerlukan biaya yang mahal dalam pembuatannya.

Penelitian telah dikembangkan dalam pengembangan metode untuk melakukan identifikasi sidik jari. Salah satu metode yang dikembangkan adalah dengan mengambil secara utuh satu citra dibandingkan dengan citra database (*global level*). Hal tersebut tentunya mengakibatkan komputasi yang tinggi karena membandingkan seluruh data piksel pada citra. Disisi lain, citra sidik jari tidak mudah dibedakan karena sulit untuk mendapatkan seluruh *singular point* dan formulasi matematika dari pola ridge menjadi sangat kompleks sehingga metode tersebut memerlukan kinerja perangkat keras yang cukup tinggi[2]. Cara lain dalam identifikasi sidik jari yaitu dengan melakukan ekstraksi fitur minutiae (*local level*) yang kemudian fitur tersebut akan menjadi entitas khusus dalam membedakan kepemilikan dari sidik jari. Sebagian besar pendekatan identifikasi sidik jari dalam empat dekade terakhir adalah berbasis *local level*. Hal tersebut terbukti dengan banyaknya jumlah penelitian yang dilakukan pada pendekatan ini [3]. Kong dkk (2018) melakukan penelitian dengan melakukan pendekatan dengan local level dengan cylinder code [4]. Kelemahan algoritma tersebut membutuhkan waktu lama untuk membangun dan hanya memanfaatkan fitur minutiae, sehingga sulit untuk diterapkan secara langsung untuk pencocokan sidik jari parsial[4]. Penelitian yang dilakukan oleh Sanchez (2018) dkk mengaplikasikan beberapa metode minutiae baik dalam ekstraksi ciri maupun *matching* membuktikan bahwa identifikasi dengan minutiae menghasilkan performa yang cukup baik dari sudut komputasi dengan parallel programming [5]. Dabouei dkk (2018) melakukan penelitian yang berbeda dimana penelitian tersebut berfokus pada pre-processing sebelum proses *minutiae extraction* [6]. Model matematika berdasarkan *Deep convolutional Neural Network* (DCNN) digunakan untuk menemukan parameter distorsi yang akurat dari citra masukan sehingga citra masukan lebih baik dan mudah untuk diekstraksi. Penelitian dalam metode meningkatkan citra masukan untuk deteksi minutiae dilakukan oleh [7]. Dalam penelitian tersebut dilakukan evaluasi kinerja dari algoritma peningkatan gambar menggunakan berbagai proses ekstraksi minutiae. Hasil dari penelitian tersebut membuktikan bahwa algoritma berbasis filter Gabor lebih baik daripada algoritma yang lain.

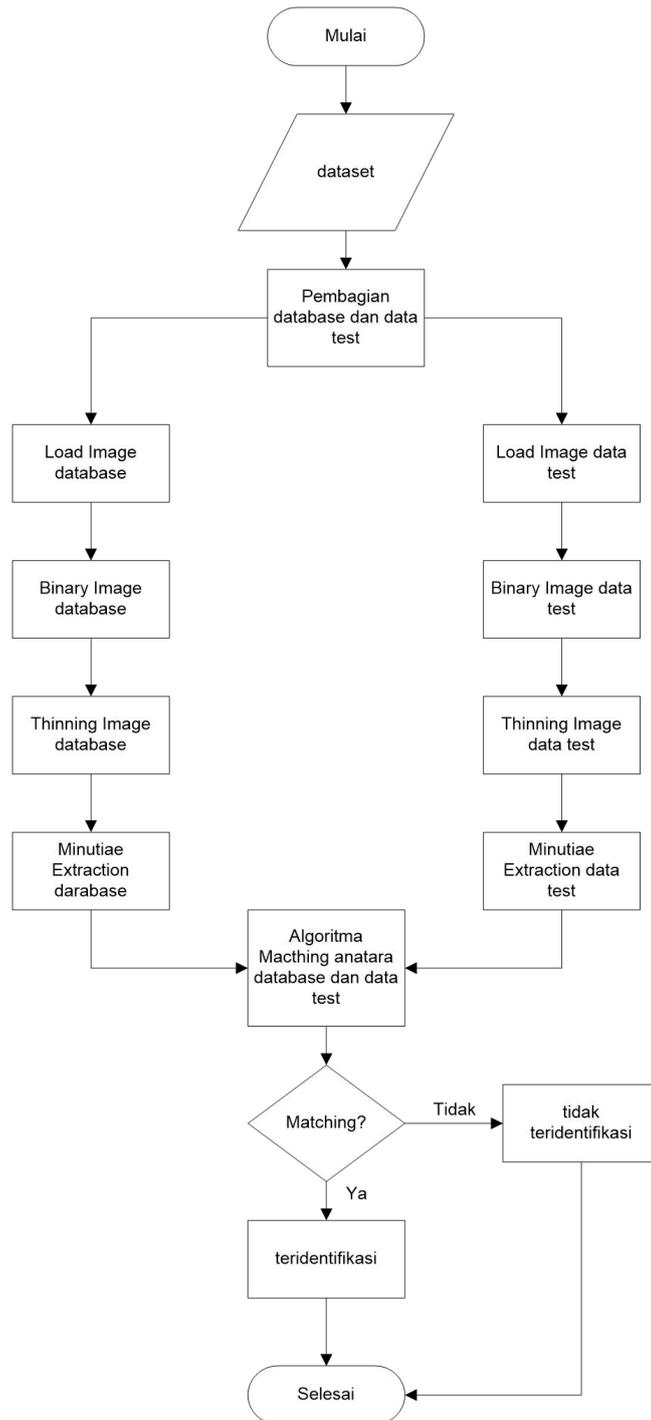
Dari sudut proses ekstraksi minutiae setelah pengolahan citra masukan, penelitian dilakukan oleh [2] yang menyatakan bahwa penambahan fitur pada ekstraksi minutiae akan meningkatkan akurasi secara signifikan. Beberapa penelitian juga telah dikembangkan dalam ekstraksi fitur ataupun matching score. Masing-masing algoritma identifikasi sidik jari memiliki kelemahan dan kekurangan yang menjadi trade-off antara efektivitas dan ketepatan [3]. Di sisi lain, identifikasi sidik jari penting mempunyai proses bahwa gambar sidik jari harus dibandingkan dengan setiap pola dalam database, sehingga akan menjadi time consuming dan membutuhkan spesifikasi hardware yang tinggi ketika dihadapkan dengan database sangat besar [8]. Dalam penelitian akan berfokus menambahkan satu fitur yang berbeda dengan hipotesis untuk meningkatkan akurasi dari algoritma yang telah dikembangkan dengan data set standar DB1.

Organisasi dari tulisan ini disusun sesuai berikut ini. Bagian II menjelaskan mengenai algoritma yang dikembangkan dalam mengekstraksi fitur serta matching fitur. Kemudian dilanjutkan dengan Bagian III yang akan membahas mengenai hasil pengujian, analisis, dan diskusi dari hasil pengujian yang diperoleh. Bagian terakhir dari tulisan ini akan memberikan kesimpulan dan penelitian selanjutnya terkait dengan otentifikasi menggunakan sidik jari.

## 2. FINGERPRINT DENGAN MINUTIAE MACTHING

Dalam melakukan otentifikasi dengan menggunakan sidik jari, citra yang diperoleh dari sensor sidik jari akan diekstraksi dan akan diidentifikasi kekhasan fiturnya [4]. Minutiae merupakan fitur dalam sidik jari yang masing-masing manusia mempunyai karakteristik minutiae yang berbeda. Hal tersebut yang menjadi konsep dasar otentifikasi menggunakan sidik jari. Diagram blok dalam proses otentifikasi dengan minutiae *matching* seperti pada Gambar 1.

Proses awal dilakukan dengan mengumpulkan data set citra dari database standar internasional. Masing-masing data set tersebut akan dibagi menjadi dua yaitu data test dan data training. Setelah itu akan dilakukan dua proses sebelum memasuki ke tahap minutiae matching.



Gambar 1. Diagram blok otentifikasi dengan minutiae *matching*

### 2.1. Citra Binari

Kedua data berupa citra tersebut akan diubah menjadi citra biner yang bernilai 0 dan 1 sehingga berwarna hitam dan putih. Pemodelan matematis dari citra biner dapat dituliskan pada persamaan berikut ini [10].

$$B(x,y) = \begin{cases} 1, & I(x,y) > T \\ 0, & I(x,y) \leq T \end{cases} \quad (1)$$

dimana  $I(x,y)$  adalah piksel citra pada posisi  $(x,y)$  dan  $T$  adalah thresholding yang digunakan besaran nilai suatu piksel untuk dikategorikan bernilai 1 atau 0.

## 2.2. Citra Thinning

*Thining* image akan diaplikasikan setelah binary citra terbentuk sehingga citra akan berbentuk sekeleton sehingga akan memudahkan untuk melakukan proses ekstraksi ciri. Secara sederhana citra thinning dapat dipahami sebagai proses dalam menghilangkan piksel hitam. Hal tersebut dapat dijelaskan sebagai berikut.

p9	p2	p3
p8	p1	p4
p7	p6	p5

Gambar 2. Piksel 3x3 yang berwarna hitam

$$X_H(p) = \sum_{i=1}^4 b_i \quad (2)$$

dimana

$$b_i = \begin{cases} 1, & \text{jika } x_{2i-1} = 0 \text{ dan } (x_{2i} = 1 \text{ atau } x_{2i+1} = 1) \\ 0, & \text{yang lainnya} \end{cases}$$

*Crossing number* didefinisikan sebagai berapa jumlah melintas dari piksel berwarna putih ke hitam, maka notasi  $X_H(p)$  sama dengan jumlah komponen hitam ketika  $p$  mempunyai keempat piksel terdekat berwarna hitam. Apabila *crossing number* bernilai 0 maka dikategorikan sebagai piksel yang terisolasi. Jika  $X_H(p)=1$ , menghapus piksel  $p$  tidak akan mengubah pola [9].

## 2.3. Ekstraksi Minutiae

Pola ridge diekstrak secara detail membuat sidik jari berbeda pada tiap orang. Pola ridge yang biasanya digunakan dalam representasi sidik jari adalah ridge end dan ridge bifurcations seperti pada Gambar 3. Secara sederhana, ridge bifurcation merupakan percabangan dari pola ridge dan ridge ending adalah akhir dari pola ridge. Pseudocode identifikasi ridge bifurcation dan ridge ending dapat dijelaskan sebagai berikut

### Pseudocode ridge bifurcation dan ridge ending

```

Input -> citra thinning
For i = 1 : jumlah baris
  For j = 1 : jumlah kolom

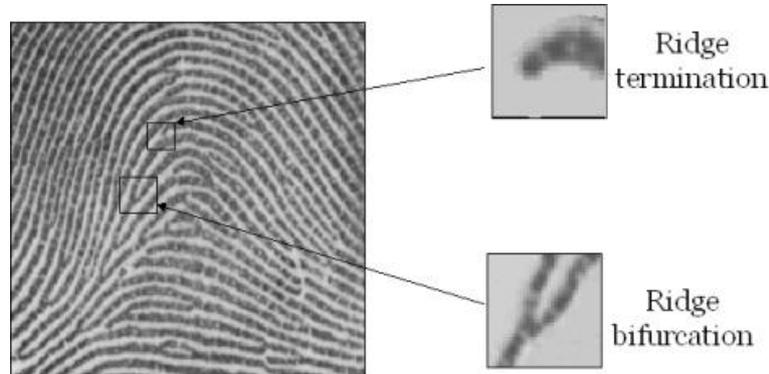
%% RIDGE BIDURCATION
  Jika i = j
    Periksa piksel p2, p3, p4, p5, p6
    Beri bobot 1 apabila salah satu piksel p1, p2, p3, p4, p5, p6 = 255
    Jumlah bobot total piksel terdekat
    Jika bobot = 3 maka ridge bifurcation

%%RIDGE ENDING
  Jika i = j
    Periksa piksel p2, p3, p4, p5, p6
    Beri bobot 1 apabila salah satu piksel p1, p2, p3, p4, p5, p6 = 255
    Jumlah bobot total piksel terdekat
    Jika bobot = 1 maka ridge end

  End
End

```

Dari pseudocode di atas, dapat disimpulkan bahwa dengan melakukan satu kali *loop* pemrograman untuk memeriksa setiap piksel pada citra dapat mengekstraksi fitur ridge bifurcation dan ridge end. Dalam program, tiap piksel mempertimbangkan 8 piksel di sekitarnya dan menghitung jumlah piksel bernilai “1” disekitarnya. Apabila berjumlah 2 maka dapat disimpulkan bahwa piksel tersebut merupakan ridge dan apabila berjumlah 1 piksel tersebut merupakan ridge ending. Hasil dari pseudocode di atas, dapat diilustrasikan pada Gambar 3.



Gambar 2. Contoh Minutiae [11]

### 2.3. Minutiae Matching

Langkah terakhir dalam proses identifikasi sidik jari adalah dengan membandingkan data test dan database yang ada. Pada penelitian ini, proses perbandingan yang disebut sebagai *minutiae matching* menggunakan Euclidean distance yaitu membandingkan posisi ridge bifurcation dan ridge end antara citra data test dan citra data base yang terekstrasi. Metode matching dengan Euclidean *distance* dapat dirumuskan seperti pada persamaan di bawah ini.

$$E_{Bi} = \sqrt{(I_{B1}(x,y) - I_{B2}(x,y))^2} \quad (3)$$

$$E_{Ei} = \sqrt{(I_{E1}(x,y) - I_{E2}(x,y))^2}, \quad (4)$$

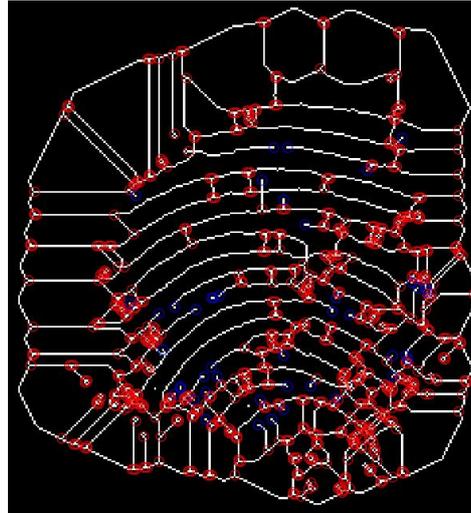
dimana  $E_{Bi}$  adalah Euclidean distance antara dua citra yang mempunyai fitur ridge bifurcation dan  $E_{Ei}$  adalah Euclidean distance antara dua citra yang mempunyai fitur ridge end yang sama. Threshold method digunakan sebagai nilai kedekatan minimal antara dua citra yang mempunyai kemiripan. Pada penelitian ini menggunakan nilai besaran threshold sebesar 15. Jika nilai  $E_{Bi}$ ,  $E_{Ei} >$  nilai threshold maka fitur dianggap mempunyai kemiripan dan diberikan skor “1”. Sehingga skor akan terus bertambah apabila ditemui nilai perbandingan fitur mempunyai nilai yang lebih besar dari threshold. Dan apabila terjadi sebaliknya maka skor akan diberikan nilai “0”.

$$T = \frac{\text{Jumlah Skor Ridge Bifurcation}}{D_B} + \frac{\text{Jumlah Skor Ridge End}}{D_E}, \quad (5)$$

dimana T adalah nilai yang diperoleh berdasarkan jumlah ridge bifurcation atau ridge yang mempunyai kemiripan melebihi nilai threshold.  $D_B$  dan  $D_E$  adalah besaran matriks data ridge bifurcation atau ridge ending. Untuk lebih meningkatkan akurasi, dalam penelitian ini, ditambahkan persamaan berikut ini.

$$P = \frac{\sum_{i=0}^n T}{\text{Jumlah Data Citra}} \quad (6)$$

Variabel P adalah jumlah skor ridge bifurcation dan ridge end pada semua citra database dibagi dengan jumlah citra database pada sidik jari orang yang sama. Metode threshold pada persamaan (6) diterapkan untuk mengidentifikasi kemiripan dengan seluruh citra pada database pada sidik jari orang yang sama.



Gambar 3. Contoh hasil source code identifikasi ridge bifurcation dan ridge ending, lingkaran merah adalah ridge bifurction dan lingkaran biru adalah ridge ending

### 3. PENGUJIAN DAN ANALISIS

#### 3.1. Hasil Pengujian

Penelitian ini menggunakan data offline dengan database standar DB1. Data yang dipergunakan berjumlah 10 orang dengan masing-masing orang mempunyai 8 database data sehingga total data sidik jari yang digunakan adalah 80 data. Data dari orang yang sama akan diambil sampling secara random kemudian dibandingkan dengan database sidik jari orang yang sama dan sidik jari orang yang berbeda. Pengujian dilakukan sebanyak 32 kali dengan data sidik jari orang yang berbeda-beda. Dengan menggunakan perangkat lunak Octave data test akan diuji dengan database dengan citra pada milik orang yang sama. Nilai thresholding yang digunakan untuk menentukan besaran jarak minimum kemiripan fitur adalah 15 dan 0.1. Contoh hasil pengujian tersebut dapat dilihat pada Tabel 1.

Tabel 1. Contoh Hasil Pengujian

Citra Datatest	Citra database	Nilai	Penilaian	Hasil
101_1	101_2- 101_10	0.103856	Sidik jari yang sama	Benar
	102_1- 102_10	0.063261	Sidik jari yang berbeda karena nilai kurang dari 0.1	Benar
	105_1- 105_10	0.13517	Sidik jari berbeda tetapi sistem mendeteksi bahwa sidik jari sama karena lebih besar dari 0.1	Salah

Tabel 1 pada percobaan yang pertama adalah membanding data 101\_1 dengan data 101\_2 sampai 101\_8 dimana memperoleh nilai 0.1 sehingga system mengatakan bahwa sidik jari 101\_1 sampai 101\_8 adalah sidik jari yang sama. Percobaan kedua, sidik jari 101\_1 dibandingkan dengan sidik jari 102\_1 sampai 102\_10 dan sistem mengatakan bahwa sidik jari berbeda. Dalam hal kedua percobaan tersebut sistem telah menunjukkan hasil yang tepat. Hasil yang salah disimpulkan oleh system adalah percobaan yang ketiga dimana system mengatakan sidik jari yang sama karena nilainya diatas 0.1 tetapi kenyataannya merupakan sidik jari yang berbeda. Percobaan seperti contoh Tabel 1 dilakukan sebanyak 32 kali dan diperoleh hasil dimana 26 kali system menyimpulkan benar dan 8 kali sistem melakukan kesalahan sehingga diperoleh akurasi sebesar

$$Acc = \frac{26}{32} \times 100\% = 81.25\%. \quad (7)$$

### 3.2. Analisis

Dari data yang diperoleh dapat dilakukan analisis terhadap kekurangan dari sistem yang ada, data yang kurang baik yang diperoleh dari 107 dan 110 sama sekali tidak dapat dilakukan deteksi ridge bifurcation dan ridge ending sehingga selalu dianggap berbeda dengan semua sidik jari yang lain. Untuk itu, *pre-processing image* harus dilakukan untuk dapat mengekstraksi data secara optimal sehingga ridge bifurcation dan ridge ending dapat terdeteksi secara baik. Selain itu, dari hasil yang diperoleh terlihat bahwa proses *thinning image* yang dihasilkan kurang optimal. Untuk mengatasi masalah tersebut, maka metode *thinning image* perlu dilakukan modifikasi agar memperoleh citra skeleton yang lebih baik. Sehingga, saat proses minutiae matching dapat lebih optimal.

### 4. KESIMPULAN

Proses otentifikasi dengan fingerprint memerlukan beberapa tahapan yaitu: pengubahan citra RGB menjadi greyscale yang kemudian dilanjutkan dengan penerapan metode threshold untuk memperoleh citra biner. Langkah selanjutnya adalah aplikasi metode *thinning image* untuk mendapatkan citra skeleton. Hasil dari citra skeleton akan diekstraksi untuk mendapatkan fitur khas ridge bifurcation dan ridge end pada setiap sidik jari. Proses final yang dilakukan dalam otentifikasi sidik jari adalah minutiae matching dengan membandingkan fitur bifurcation dan ridge antara data tes dan database. Pada penelitian ini, ditambahkan *average Euclidean Distance* dari seluruh dataset pada sidik jari orang yang sama untuk memperoleh probabilitas yang tinggi terhadap identifikasi sidik jari pada orang yang sama maupun tidak sehingga sistem dapat memberikan kesimpulan yang lebih akurat. Hasil pengujian menunjukkan bahwa akurasi dari metode yang diusulkan adalah sebesar 81% melalui 32 kali percobaan. Kelemahan dari metode yang digunakan adalah adanya citra yang tidak dapat diekstraksi fitur baik ridge bifurcation maupun ridge end sehingga memerlukan *pre-processing image*. Selain itu, aplikasi dari metode *thinning* kurang optimal sehingga masih terdapat piksel yang bukan merupakan bifurcation tetapi teridentifikasi sebagai bifurcation. Pada penelitian selanjutnya akan dilakukan metode filtering agar menghasilkan citra skeleton yang lebih baik disertai *pre processing image* agar citra yang kurang bagus dapat diperbaiki dan memperoleh fitur ekstraksi yang baik.

### DAFTAR PUSTAKA

- [1] Ravi, J, K. B. Fingerprint Recognition using Minutia Score Matching. *International Journal of Engineering Science and Technology*. 2009; 1(2):35-42.
- [2] Qiongxu Li, C. J.. *Multi-feature based score fusion method for Fingerprint Recognition Accuracy Boosting*. Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA). 2016.
- [3] Daniel Peraltaa, M. G. *A Survey on Fingerprint Minutiae-based Local Matching for Verification and Identification: Taxonomy and Experimental Evaluation*. *Information Sciences*. 2015; 315:67-87.
- [4] Xiangwen Kong, Y. W. *A Cylinder Code-Based Partial Fingerprint Matching Algorithm for Small Fingerprint Scanners*. 13th Chinese Conference, CCBP. China. 2018.
- [5] Andres Jesus Sanchez, L. F.-P. *A First Step to Accelerating Fingerprint Matching Based on Deformable Minutiae Clustering*. *Lecture Notes in Computer Science*. 2018; 11160:361-317.
- [6] Ali Dabouei, H. K. *Fingerprint Distortion Rectification using Deep Convolutional Neural Networks*. 2018. Retrieved from arXiv: 1801.01198v1 [cs.CV]
- [7] Malwade, A. R. *Survey on Enhancement Technique to Improve Accuracy in Fingerprint Matching*. *International Journal of Advanced Research in Computer Science and Software Engineering*. 2015; 5(2):28-32.
- [8] Asfiya siddiqui, S. S. *Fingerprint Feature Extractors Using Multiple Machine Learning: A Comparative In The Study*. *International Journal of Scientific and Technology Research*. 2019; 8(7).
- [9] Louisa Lam, S.-W. L. *Thinning Methodologies - A Comprehensive Survey*. *IEEE Transaction on Pattern Analysis and Machine Intelligence*. 1992; 14(9):869-885.
- [10] Pankanti, R. M. *Fingerprint Minutiae: A Constructive Definition*. *International Workshop on Biometric Authentication*. 2002; 58-66.
- [11] (n.d.). Retrieved from <https://www.griaulebiometrics.com/pt-br/book/understanding-biometrics/types/description>.