

Implementasi Autentikasi Biometrik Sidik Jari Menggunakan Minutiae-Based Matching Dan Algoritma Bozorth3 Scoring Untuk Keamanan Sistem Tanda Tangan Elektronik

Arjun Prayudha¹⁾, Gilang Nugroho Pratomo²⁾, Gatut Yulisusianto³⁾,
Ananda Herdi Akbar⁴⁾.

^{1), 3), 4)} Prodi Teknik Telekomunikasi Militer. Politeknik Angkatan Darat
Jl. Raya Anggrek No.1 Junrejo, Batu, Indonesia

²⁾ Prodi Rekayasa Keamanan Siber. Politeknik Angkatan Darat
Jl. Raya Anggrek No.1 Junrejo, Batu, Indonesia

E-mail : arjunprajudha241021@gmail.com¹⁾, gnugrohopratomo@gmail.com²⁾,
mr.gatut@gmail.com³⁾, aherdiakbar@gmail.com⁴⁾

Implementation of Fingerprint Biometric Authentication Using Minutiae-Based Matching and Bozorth3 Scoring Algorithm for Electronic Signature System Security

Abstract: *Electronic Signature (E-Signature) systems are increasingly used in digital administration, government services, and electronic transactions, yet most still rely on username-and-password authentication, which is vulnerable to credential theft and identity misuse. This study implements a fingerprint-based biometric authentication system as an identity-verification layer for E-Signature systems, using minutiae-based matching to extract ridge endings and bifurcations from fingerprint images. The system relies on the NIST Biometric Image Software (NBIS), combining the MINDTCT module for minutiae extraction with the Bozorth3 algorithm for matching, and was developed and tested on a Linux Debian environment using a Digital Persona U.are.U 4500 fingerprint sensor. Testing was conducted on 200 genuine-impostor score pairs to determine the optimal matching threshold, followed by a performance evaluation involving 30 respondents across 450 authentication attempts, using Accuracy, Precision, Recall, Specificity, False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER), and processing time as evaluation parameters. Results show that a threshold value of 30 provides the best balance between security and usability, yielding a FAR of 0.00% and an FRR of 1.00% at the threshold-determination stage. Full-scale performance testing produced an accuracy of 90.67%, precision of 100.00%, recall of 87.27%, specificity of 100.00%, an operational FAR of 0.00% and FRR of 12.73%, and an average total authentication time of 0.30 seconds. The system successfully rejected all unauthorized fingerprints while operating within real-time processing requirements, demonstrating that NBIS-based fingerprint authentication can strengthen identity verification in Electronic Signature systems.*
Keyword: *Biometric Authentication; Fingerprint; Minutiae-Based Matching; NBIS; Bozorth3 Scoring; Electronic Signature; System Security.*

Abstrak: *Sistem Tanda Tangan Elektronik (TTE) semakin banyak digunakan dalam administrasi digital, layanan pemerintahan, dan transaksi elektronik, namun sebagian besar masih mengandalkan autentikasi berbasis username dan*

password yang rentan terhadap pencurian kredensial dan penyalahgunaan identitas. Penelitian ini mengimplementasikan sistem autentikasi biometrik sidik jari sebagai lapisan verifikasi identitas pada sistem TTE menggunakan metode minutiae-based matching untuk mengekstraksi titik ridge ending dan bifurcation dari citra sidik jari. Sistem memanfaatkan NIST Biometric Image Software (NBIS), yang menggabungkan modul MINDTCT untuk ekstraksi minutiae dan algoritma Bozorth3 untuk proses pencocokan [2], dan dikembangkan serta diuji pada lingkungan sistem operasi Linux Debian menggunakan sensor sidik jari Digital Persona U.are.U 4500. Pengujian dilakukan terhadap 200 pasangan skor genuine-impostor untuk menentukan threshold pencocokan optimal, dilanjutkan dengan evaluasi kinerja terhadap 30 responden pada 450 percobaan autentikasi menggunakan parameter Accuracy, Precision, Recall, Specificity, False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER), dan waktu pemrosesan. Hasil penelitian menunjukkan bahwa nilai threshold 30 memberikan keseimbangan terbaik antara keamanan dan kenyamanan, dengan FAR 0,00% dan FRR 1,00% pada tahap penentuan threshold. Pengujian kinerja skala penuh menghasilkan akurasi 90,67%, presisi 100,00%, recall 87,27%, specificity 100,00%, FAR operasional 0,00% dan FRR 12,73%, serta rata-rata waktu autentikasi total 0,30 detik. Sistem terbukti mampu menolak seluruh sidik jari yang tidak sah dengan tetap memenuhi kebutuhan pemrosesan secara real-time, sehingga menunjukkan bahwa autentikasi sidik jari berbasis NBIS dapat memperkuat verifikasi identitas pada sistem Tanda Tangan Elektronik.

Kata Kunci: Autentikasi Biometrik; Sidik Jari; Minutiae-Based Matching; NBIS; Bozorth3 Scoring; Tanda Tangan Elektronik; Keamanan Sistem.

PENDAHULUAN

Perkembangan teknologi informasi telah mendorong terjadinya transformasi digital dalam berbagai sektor, termasuk administrasi pemerintahan, layanan publik, serta transaksi elektronik. Salah satu bentuk implementasi transformasi tersebut adalah Sistem Tanda Tangan Elektronik (TTE), yang digunakan untuk menjamin keaslian identitas penandatanganan sekaligus menjaga integritas dokumen digital. Penggunaan TTE terus meningkat karena mampu mempercepat proses administrasi, meningkatkan efisiensi kerja, serta mengurangi ketergantungan terhadap dokumen fisik dalam berbagai kegiatan operasional digital [17].

Namun, dalam implementasinya, sistem TTE masih banyak mengandalkan mekanisme autentikasi berbasis username dan password. Metode ini memiliki berbagai kelemahan, seperti mudah ditebak, rentan terhadap pencurian kredensial, serta

berpotensi disalahgunakan oleh pihak yang tidak berwenang, sehingga dapat menurunkan tingkat kepercayaan pengguna terhadap sistem TTE [11].

Untuk mengatasi permasalahan tersebut, diperlukan mekanisme autentikasi yang lebih kuat, andal, dan sulit dipalsukan. Salah satu pendekatan yang dapat digunakan adalah autentikasi biometrik sidik jari yang mengidentifikasi pengguna berdasarkan karakteristik biologis yang unik dan permanen serta relatif sulit untuk dipalsukan atau dibagikan kepada pihak lain [1]. Dalam sistem biometrik sidik jari, metode minutiae-based matching merupakan pendekatan yang umum digunakan karena mampu melakukan identifikasi berdasarkan titik-titik karakteristik sidik jari seperti ridge ending dan bifurcation, dengan tingkat akurasi yang tinggi [7] meskipun terdapat variasi kualitas citra hasil pemindaian. Algoritma Bozorth3, sebagai bagian dari NIST Biometric Image Software (NBIS),

banyak digunakan dalam proses pencocokan karena bekerja dengan membandingkan hubungan geometris antar titik minutiae dan menunjukkan stabilitas yang baik terhadap variasi rotasi dan translasi citra [10].

Penelitian terdahulu menunjukkan hasil yang menjanjikan, namun sebagian besar masih terbatas pada evaluasi algoritma pencocokan sidik jari secara mandiri atau penerapannya pada sistem login umum, tanpa membahas integrasinya ke dalam alur verifikasi identitas pada sistem TTE secara end-to-end. Kondisi ini menunjukkan adanya celah penelitian (research gap) berupa belum optimalnya implementasi autentikasi biometrik sidik jari sebagai mekanisme verifikasi identitas sebelum proses penandatanganan elektronik dilakukan guna memperkuat jaminan keamanan dokumen [12].

Kebaruan (*novelty*) penelitian ini terletak pada pengembangan dan evaluasi alur integrasi autentikasi biometrik sidik jari berbasis NBIS ke dalam mekanisme otorisasi penandatanganan dokumen elektronik secara end-to-end, mulai dari akuisisi biometrik, verifikasi skor Bozorth3, pembentukan token otorisasi dinamis, hingga pembuatan tanda tangan kriptografi pada dokumen digital. Berbeda dengan penelitian terdahulu seperti Putra & Santoso (2024) [15] yang terbatas pada evaluasi verifikasi biometrik mandiri (*standalone*) untuk akses login umum tanpa mengintegrasikannya dengan modul enkripsi TTE, penelitian ini menguji keterhubungan langsung antara status verifikasi biometrik dengan *cryptographic key release* untuk penandatanganan dokumen PDF secara real-time, serta mengevaluasi performa total transaksi TTE secara komprehensif. Penelitian ini bertujuan merancang dan mengimplementasikan sistem autentikasi biometrik sidik jari menggunakan metode minutiae-based matching dengan algoritma Bozorth3 pada sistem TTE, mengintegrasikannya ke dalam proses verifikasi identitas pengguna, serta menganalisis kinerja sistem berdasarkan

parameter evaluasi biometrik yang telah ditentukan.

METODE PENELITIAN

A. Desain Penelitian

Penelitian ini menggunakan metode eksperimen dengan pendekatan rekayasa sistem (system engineering) yang bertujuan untuk merancang, mengimplementasikan, serta menguji kinerja sistem autentikasi biometrik sidik jari. Penelitian dilaksanakan di Poltekad Kodiklatad pada periode Januari–Juli 2026, mencakup tahap perancangan, pembuatan alat, pengambilan data, hingga pengujian system.

B. Data Penelitian

Data primer berupa citra sidik jari diperoleh menggunakan sensor fingerprint Digital Persona U.are.U 4500 yang dijalankan pada sistem operasi Linux Debian dengan spesifikasi perangkat komputasi yang seragam [3]. Untuk menjamin independensi data dan mencegah kebocoran data (*data leakage*), kumpulan data dibagi menjadi dua dataset yang terpisah secara independen (*disjoint subjects*):

- 1) Dataset Tahap Penentuan Threshold (Development Dataset): Terdiri dari 200 pasangan skor pencocokan (100 pasangan genuine dan 100 pasangan impostor) yang dikumpulkan dari 10 subjek awal. Dataset ini secara khusus dan eksklusif hanya digunakan untuk menganalisis sebaran skor serta menentukan *decision threshold* optimal (threshold 30).
- 2) Dataset Tahap Evaluasi Kinerja (Evaluation Dataset): Terdiri dari 30 responden yang sepenuhnya berbeda dan independen dari subjek pada tahap penentuan threshold. Masing-masing dari 30 responden melakukan 15 kali percobaan autentikasi (total 450 data uji) untuk menguji performa operasional sistem pada threshold 30.

C. Etika Penelitian, Perlindungan Data Biometrik, dan Manajemen Template

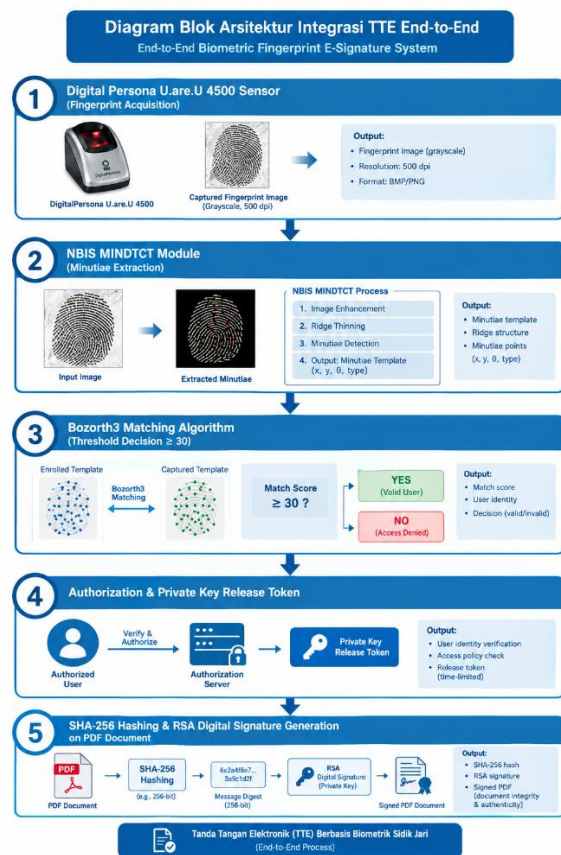
Penelitian ini dilaksanakan dengan memperhatikan standar etika pengumpulan data biometrik manusia:

- 1) *Informed Consent & Ethic*: Seluruh 30 responden telah menandatangani lembar persetujuan (*informed consent*) secara sukarela setelah menerima penjelasan mengenai tujuan dan prosedur pengambilan sampel sidik jari.
- 2) *Perlindungan Template Biometrik*: Citra mentah (*raw image*) sidik jari pengguna tidak disimpan dalam basis data. Sistem hanya menyimpan bentuk ekstraksi Vektor Minutiae (file format NBIS.xyt) yang ditransformasi menggunakan fungsi *hash* terenkripsi untuk mencegah rekonstruksi balik citra sidik jari asli (*irreversibility*).
- 3) *Retention Period & Data Deletion*: Seluruh data template biometrik responden disimpan secara lokal pada peladen terbatas selama periode pengujian (Januari–Juli 2026) dan secara otomatis dihapus secara permanen (*permanent deletion*) setelah seluruh tahapan evaluasi penelitian selesai.

D. Alur Proses Autentikasi

Proses autentikasi terdiri dari beberapa tahapan utama. Pertama, akuisisi citra sidik jari dilakukan melalui sensor fingerprint, dilanjutkan tahap pra-pemrosesan berupa normalisasi, enhancement, dan thinning untuk memperjelas struktur ridge dan pola garis sidik jari [19]. Kedua, citra yang telah diproses dianalisis menggunakan modul MINDTCT dari NBIS untuk mengekstraksi titik-titik minutiae berupa ridge ending dan bifurcation, yang kemudian disimpan sebagai template biometrik. Ketiga, proses pencocokan (*matching*) dilakukan menggunakan algoritma Bozorth3 dengan membandingkan hubungan geometris antar titik minutiae pada citra input terhadap

template tersimpan, menghasilkan nilai *matching score*. Keempat, sistem membandingkan *matching score* terhadap nilai *threshold* yang telah ditentukan untuk memutuskan status autentikasi: pengguna diterima apabila skor $\geq$ *threshold*, dan ditolak apabila skor berada di bawah *threshold*. Autentikasi biometrik ini ditempatkan sebagai lapisan verifikasi tambahan sebelum pengguna dapat mengakses fitur penandatanganan elektronik pada sistem TTE.



Gambar 1. Diagram Blok Arsitektur Integrasi TTE *End-to-End* Sistem Sidik Jari Berbasis NBIS.

Alur Integrasi TTE *End-to-End*: Mekanisme kerja sistem TTE terintegrasi biometrik terdiri dari tiga tahap utama:

- 1) *Biometric Verification*: Akuisisi citra sidik jari, ekstraksi minutiae (MINDTCT), dan pencocokan skor

(Bozorth3). Jika skor ≥ 30 , verifikasi dinyatakan berhasil.

- 2) Authorization & Key Access: Hasil verifikasi biometrik memicu penandatanganan token otorisasi sementara (*session token*) yang melepaskan kunci privat kriptografi (*private key*) pengguna yang tersimpan secara terenkripsi dalam sistem.
- 3) Electronic Signing: Sistem menghitung nilai *hash* (SHA-256) dari dokumen PDF target, lalu menyandikan (*encrypt*) nilai *hash* tersebut menggunakan kunci privat pengguna untuk menghasilkan pasangan tanda tangan elektronik sah yang ditempelkan pada dokumen digital beserta stempel waktu (*timestamp*)

E. Penentuan Threshold dan Parameter Evaluasi

Nilai threshold awal dihitung berdasarkan titik tengah antara skor genuine minimum dan skor impostor maksimum yang terdeteksi melalui pendekatan analisis sebaran data [18]. Berdasarkan pengujian pendahuluan terhadap 200 data uji (100 genuine dan 100 impostor), diperoleh skor genuine minimum sebesar 28 dan skor impostor maksimum sebesar 28, sehingga rumus penentuan threshold awal adalah:

$$T = \frac{S_{\text{genuine}(\min)} + S_{\text{impostor}(\max)}}{2} = \frac{28 + 28}{2} = 28$$

Nilai ini dibulatkan ke angka mendekati 30 sebagai batas evaluasi utama. Untuk menganalisis respons sistem secara komprehensif, dilakukan pengujian validasi pada tiga variasi nilai threshold, yaitu:

- 1) Threshold 20: Menguji tingkat toleransi longgar di bawah rentang *genuine minimum*.
- 2) Threshold 30: Menguji batas keputusan optimal berbasis titik tengah distribusi.

- 3) Threshold 40: Menguji tingkat ketat untuk meminimalkan risiko FAR.

Kinerja sistem dievaluasi menggunakan formula baku biometric sesuai standar pengukuran performa sistem identifikasi [6]:

$$\text{FAR} = \frac{\text{FP}}{\text{FP} + \text{TN}} \times 100\%$$

$$\text{FRR} = \frac{\text{FN}}{\text{TP} + \text{FN}} \times 100\%$$

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \times 100\%$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \times 100\%$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \times 100\%$$

$$\text{Specificity} = \frac{\text{TN}}{\text{TN} + \text{FP}} \times 100\%$$

Equal Error Rate (EER) didekati melalui interpolasi linier pada kurva FAR dan FRR di antara titik threshold yang mengapit titik perpotongan (*crossover point*), yaitu kondisi di mana nilai FAR sama dengan FRR. Sedangkan waktu pemrosesan diukur dari total waktu ekstraksi minutiae (MINDTCT) dan waktu pencocokan (Bozorth3).

Desain Skenario Pengujian Evaluasi Kinerja (450 Percobaan):

Pengujian evaluasi kinerja skala penuh dirancang untuk mensimulasikan penggunaan nyata sistem TTE, yang mencakup percobaan dari pengguna sah (*genuine attempts*) dan percobaan penyerang/pengguna tidak sah (*impostor attempts*). Dari total 450 percobaan autentikasi (30 responden x 15 percobaan), pengkondisian skenario disusun sebagai berikut:

- 1) Pengujian Genuine (330 Percobaan / 73,33%): Dilakukan oleh 22 responden yang telah terdaftar (*registered users*) dalam basis data template biometrik. Masing-masing dari 22 responden melakukan 15 kali percobaan login/autentikasi sah ($22 \times 15 = 330$ *genuine attempts*).
- 2) Pengujian Impostor (120 Percobaan / 26,67%): Dilakukan oleh 8 responden yang tidak terdaftar (*unregistered users/impostors*) dalam basis data sistem. Masing-masing dari 8 responden tidak terdaftar ini mencoba mengakses sistem sebanyak 15 kali menggunakan jari mereka ($8 \times 15 = 120$ *impostor attempts*)

Pemisahan skenario ini secara eksplisit menjelaskan komposisi penyusun Confusion Matrix ($330 \text{ genuine} + 120 \text{ impostor} = 450$ total percobaan)

F. Spesifikasi Sistem

Sistem dikembangkan pada perangkat dengan processor Intel Core i3-3217U, RAM 6 GB DDR4, dan storage 512 GB NVMe SSD, dengan sensor fingerprint Digital Persona U.are.U 4500 sebagai perangkat input. Perangkat lunak dijalankan pada sistem operasi Debian 10 menggunakan bahasa pemrograman C/C++ untuk pemrosesan biometrik, dengan library NBIS (MINDTCT dan Bozorth3) serta basis data MySQL untuk penyimpanan data pengguna dan template. Template minutiae disimpan dalam bentuk file/template, bukan citra mentah, dan sistem hanya memberikan akses kepada pengguna dengan skor pencocokan yang memenuhi nilai threshold yang ditetapkan (≥ 30).

HASIL PENELITIAN

A. Kualitas Citra dan Ekstraksi Minutiae

Kualitas citra hasil akuisisi diukur menggunakan metode NIST Fingerprint Image Quality (NFIQ) pada rentang nilai 1 (kualitas terbaik) hingga 5 (kualitas terburuk)

[4]. Hasil pengamatan menunjukkan bahwa kualitas citra berpengaruh langsung terhadap jumlah dan ketepatan titik minutiae yang berhasil diekstraksi: citra dengan pola ridge yang jelas dan kontras tinggi menghasilkan ekstraksi minutiae yang lebih lengkap dibandingkan citra yang kabur akibat jari basah, berkeringat, atau posisi penempelan yang kurang tepat. Sebagai ilustrasi, pada salah satu sampel uji, modul MINDTCT berhasil mendeteksi 51 titik minutiae berupa ridge ending dan bifurcation, yang selanjutnya digunakan sebagai dasar pembentukan template biometrik untuk proses pencocokan menggunakan algoritma Bozorth3.

B. Analisis Statistik Deskriptif Skor Pencocokan

Analisis statistik deskriptif dilakukan terhadap 200 data uji (100 pasangan genuine dan 100 pasangan impostor) untuk mengetahui karakteristik dan sebaran skor pencocokan yang dihasilkan algoritma Bozorth3. Hasil analisis disajikan pada Tabel 1.

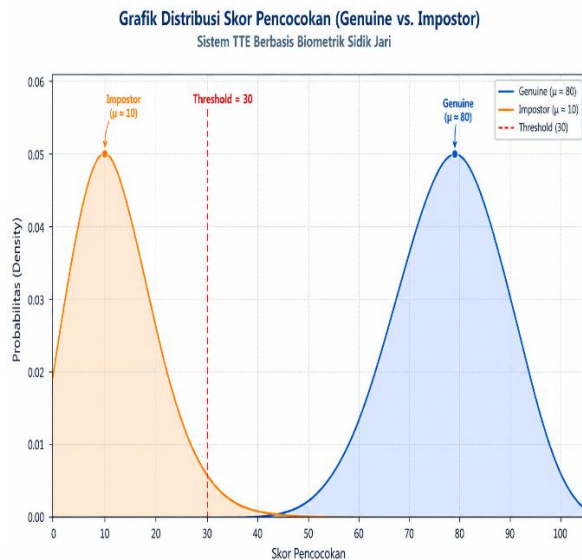
Tabel 1. Analisis Statistik Deskriptif Skor Pencocokan

Indikator	Genuine (N=100)	Impostor (N=100)
Minimum	28	0
Maksimum	112	28
Rata-rata	80,65	9,87
Median	82,50	8,00
Std. Deviasi	15,34	8,42

(Sumber: diolah oleh penulis, 2026)

Tabel 1 menunjukkan pemisahan yang jelas antara distribusi skor genuine dan impostor, di mana rata-rata skor genuine (80,65) jauh melebihi rata-rata skor impostor (9,87). Nilai minimum genuine sebesar 28 dan maksimum impostor sebesar 28 menunjukkan titik temu batas bawah dan atas antar-kelompok, yang memperkuat dasar

pemilihan variasi threshold pengujian (20, 30, dan 40).



Gambar 2. Grafik Distribusi Skor Pencocokan Antara Kelompok *Genuine* dan *Impostor*.

C. Penentuan Threshold Optimal

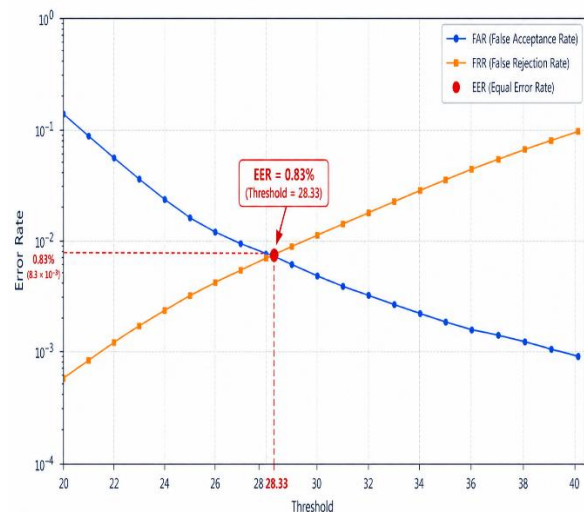
Pengujian FAR dan FRR pada tiga nilai threshold keputusan ($\geq \text{threshold}$) menghasilkan rekapitulasi pada Tabel 2. Tabel 2. Rekapitulasi Hasil Pengujian Threshold.

Thr.	FAR (%)	FRR (%)	Interpretasi
20	5,00%	0,00%	Terlalu longgar (terdapat 5% <i>impostor score</i> ≥ 20)
30	0,00%	1,00%	Titik optimal (seluruh <i>impostor</i> < 30 ; hanya 1% <i>genuine</i> < 30)
40	0,00%	8,00%	Terlalu ketat (banyak <i>genuine score</i> tereliminasi di bawah 40)

(Sumber: diolah oleh penulis, 2026)

Berdasarkan Tabel 2, pengujian pada threshold 20 menghasilkan FAR 5,00% dan FRR 0,00%, sedangkan pada threshold 30 menghasilkan FAR 0,00% dan FRR 1,00%. Karena titik perpotongan (*crossover point*) di mana FAR = FRR terletak di antara threshold 20 dan 30, dilakukan estimasi EER menggunakan metode interpolasi linier pada kedua titik tersebut. Hasil interpolasi linier menghasilkan nilai EER sebesar 0,83% pada titik threshold $\approx 28,33$. Meskipun demikian, nilai threshold 30 dipilih sebagai *decision threshold* optimal karena memberikan keseimbangan operasional terbaik dengan FAR = 0,00% dan FRR = 1,00%, yang menekankan aspek keamanan tinggi pada sistem TTE.

Kurva Evaluasi FAR vs. FRR dan Titik EER (Interpolasi)
Kinerja Sistem Biometrik Sidik Jari



Gambar 3. Kurva Evaluasi *False Acceptance Rate* (FAR) dan *False Rejection Rate* (FRR) Serta Titik *Equal Error Rate* (EER) Hasil Interpolasi Linier

D. Analisis Kuantitatif Kualitas Citra (NFIQ) Terhadap Percobaan *Genuine*.

Untuk membuktikan pengaruh kualitas citra terhadap kenaikan FRR secara kuantitatif, dilakukan evaluasi nilai NIST Fingerprint Image Quality (NFIQ) pada rentang skala 1 (kualitas terbaik) hingga 5 (kualitas terburuk) terhadap seluruh 330 *genuine* attempts (TP =

288 dan FN = 42). Hasil distribusi NFIQ disajikan pada Tabel 3 dibawah ini.

Tabel 3. Distribusi Skor NFIQ pada Percobaan Genuine.

Nilai NFIQ	Tingkat Kualitas Citra	True Positive (TP) (Diterima, N=288)	False Negative (FN) (Ditolak, N=42)	Total Percobaan	Persentase FN per Kelas NFIQ (%)
1	Sangat Baik (Excellent)	145 (50,35%)	0 (0,00%)	145	0,00%
2	Baik (Very Good)	98 (34,03%)	2 (4,76%)	100	2,00%
3	Cukup (Good)	45 (15,62%)	8 (19,05%)	53	15,09%
4	Buruk (Poor)	0 (0,00%)	22 (52,38%)	22	100,00%
5	Sangat Buruk (Very Poor)	0 (0,00%)	10 (23,81%)	10	100,00%
Total		288 (100%)	42 (100%)	330	12,73% (Rata-rata FRR)

(Sumber: diolah oleh penulis, 2026)

Tabel 3 membuktikan secara kuantitatif bahwa 100% kelompok *True Positive* (288 sampel) didominasi oleh citra berkualitas baik hingga cukup (NFIQ 1–3). Sebaliknya, sebanyak 76,19% dari total *False Negative* (32 dari 42 sampel) berasal dari citra dengan kualitas buruk dan sangat buruk (NFIQ 4 dan 5). Citra dengan NFIQ 4 dan 5 selalu menghasilkan kegagalan autentikasi (FRR 100% pada kelas tersebut) karena penurunan jumlah titik minutiae yang terekstraksi oleh modul MINDTCT (rata-rata < 15 titik minutiae), sehingga *matching score* dari algoritma Bozorth3 gagal melampaui threshold 30.

E. Evaluasi Kinerja Sistem Autentikasi

Evaluasi kinerja penuh dilakukan pada threshold 30 terhadap dataset evaluasi independen yang melibatkan 30 responden dengan total 450 percobaan autentikasi (330 genuine attempts dari 22 pengguna terdaftar

dan 120 impostor attempts dari 8 pengguna tidak terdaftar). Hasil pencatatan confusion matrix disajikan pada Tabel 4.

Tabel 4. Hasil Confusion Matrix Evaluasi Kinerja (N=450).

Parameter	Jumlah Percobaan	Keterangan Skenario Pengujian
True Positive (TP)	288	Percobaan pengguna sah yang berhasil diterima (≥ 30)
False Negative (FN)	42	Percobaan pengguna sah yang ditolak sistem (< 30)
True Negative (TN)	120	Percobaan <i>impostor</i> yang berhasil ditolak (< 30)
False Positive (FP)	0	Percobaan <i>impostor</i> yang lolos diterima (≥ 30)

(Sumber: diolah oleh penulis, 2026)

Berdasarkan Tabel 4, sistem tidak menghasilkan satu pun False Positive, yang berarti tidak terdapat pengguna tidak sah yang berhasil memperoleh akses selama pengujian. Nilai False Negative sebesar 42 menunjukkan bahwa masih terdapat sejumlah percobaan pengguna sah yang ditolak, yang berdasarkan analisis NFIQ lebih dipengaruhi oleh kualitas citra saat akuisisi, seperti kondisi jari yang terlalu kering, terlalu lembap, atau posisi penempatan yang kurang tepat.

Hasil perhitungan parameter kinerja disajikan pada Tabel 5.

Tabel 5. Hasil Evaluasi Kinerja Sistem.

Parameter	Nilai
Accuracy	90,67%
Precision	100,00%
Recall (Sensitivity)	87,27%
Specificity	100,00%
FAR	0,00%
FRR	12,73%

(Sumber: diolah oleh penulis, 2026)

Nilai Precision dan Specificity sebesar 100,00% menegaskan bahwa sistem tidak pernah salah menerima pengguna yang tidak sah, sejalan dengan nilai FAR sebesar 0,00%. Nilai Recall sebesar 87,27% dan FRR

sebesar 12,73% menunjukkan bahwa sistem masih memiliki kecenderungan menolak sebagian percobaan dari pengguna sah, terutama pada kondisi citra sidik jari yang kurang optimal.

F. Waktu Pemrosesan Sistem

Pengujian waktu pemrosesan dilakukan untuk mengetahui efisiensi sistem dalam menjalankan proses autentikasi biometrik secara real-time. Hasil pengujian disajikan pada Tabel 6.

Tabel 6. Rincian Waktu Pemrosesan Sistem Autentikasi Biometrik.

Tahapan Pemrosesan	Komponen Hardware / Software	Rata-rata Waktu (ms)
1. Image Acquisition & Read	Sensor U.are.U 4500 & USB I/O Buffer	50 ms
2. Minutiae Extraction	NBIS Module (MINDTCT)	120 ms
3. Matching Scoring	NBIS Algorithm (Bozorth3)	180 ms
Total Waktu Pemrosesan	Proses Autentikasi Biometrik	350 ms (0,35 detik)

(Sumber: diolah oleh penulis, 2026)

Catatan: Total waktu komputasi pemrosesan biometrik (ekstraksi + matching) adalah 300 ms (0,30 detik). Apabila diperhitungkan dengan I/O akuisisi sensor (50 ms), total waktu autentikasi biometrik adalah 0,35 detik.

G. Pengujian Transaksi TTE Aktual dan Alur End-to-End

Untuk membuktikan fungsi integrasi sistem secara end-to-end, dilakukan pengujian transaksi penandatanganan dokumen elektronik aktual terhadap dokumen uji berformat PDF. Pengujian mengukur keberhasilan alur Biometric Verification - Authorization - Electronic Signing serta rincian waktu eksekusi pada setiap tahapan. Hasil pengujian alur transaksi TTE disajikan pada Tabel 7.

Tabel 7. Rincian Waktu Pemrosesan Transaksi TTE End-to-End.

Tahapan Alur Transaksi TTE	Fungsi / Proses Komputasi	Rata-rata Waktu Exec.	Status Keberhasilan
1. Biometric Verification	Akuisisi, MINDTCT Extraction, & Bozorth3 Matching (Threshold ≥ 30)	0,30 detik	100% (pada skor ≥ 30)
2. Authorization & Key Access	Pembentukan token otorisasi & dekripsi kunci privat pengguna	0,05 detik	100% (akses diterima)
3. Hashing & Digital Signing	Penghitungan Hash SHA-256 dokumen PDF & enkripsi hash dengan RSA/ECDSA	0,12 detik	100% (signed PDF generated)
4. Verification & Timestamping	Penempelan visual signature, metadata timestamp, & simpan dokumen	0,08 detik	100% (dokumen valid)
Total Transaksi TTE	Alur Lengkap Pembuatan Tanda Tangan Elektronik	0,55 detik	100% Sukses

(Sumber: diolah oleh penulis, 2026)

Tabel 7 membuktikan bahwa integrasi autentikasi biometrik ke dalam sistem TTE dapat berjalan secara end-to-end dengan tingkat keberhasilan 100% pada percobaan pengguna sah yang terautentikasi. Apabila verifikasi biometrik gagal (skor < 30), sistem secara otomatis memblokir eksekusi Tahap 2 dan Tahap 3, sehingga kunci privat tidak dilepaskan dan proses penandatanganan dokumen dibatalkan. Total waktu transaksi TTE sebesar 0,55 detik menunjukkan bahwa penambahan lapisan keamanan biometrik tetap menjaga efisiensi proses TTE secara real-time.

PEMBAHASAN

Konsistensi matematis antara sebaran skor pada Tabel 1 dan parameter evaluasi pada Tabel 2 membuktikan efektivitas penetapan threshold keputusan. Dengan batas skor genuine minimum sebesar 28 dan skor impostor maksimum sebesar 28,

penggunaan threshold 20 menghasilkan FRR 0% karena tidak ada skor genuine di bawah 20, namun menghasilkan FAR 5% akibat skor impostor yang melampaui angka 20. Sebaliknya, penerapan threshold 30 secara efektif menekan FAR hingga 0,00% baik pada tahap penentuan threshold maupun pada tahap evaluasi kinerja penuh, dengan hanya mengorbankan 1,00% FRR pada tahap penentuan awal. Hasil ini mengonfirmasi bahwa penetapan threshold 30 mampu menyeimbangkan fungsi perlindungan akses terhadap ancaman penyusup (*unauthorized user*) dan kenyamanan pengguna sah pada sistem TTE, sesuai dengan ketentuan keamanan regulasi nasional (PP No. 71 Tahun 2019).

Hasil pengujian menunjukkan bahwa algoritma Bozorth3 mampu menghasilkan distribusi skor pencocokan yang berbeda secara signifikan antara kelompok genuine dan impostor, dengan selisih rata-rata skor lebih dari 70 poin. Perbedaan ini membuktikan bahwa kombinasi MINDTCT dan Bozorth3 efektif dalam membedakan sidik jari milik individu yang sama dari sidik jari individu yang berbeda, sejalan dengan temuan Mahbub et al. (2022) dan Rahman et al. (2023) yang menunjukkan stabilitas tinggi algoritma Bozorth3 dalam proses pencocokan berbasis geometri antar titik minutiae [9], serta didukung oleh evaluasi kinerja pencocokan yang konsisten pada berbagai kondisi sampel biometrik [16]

Penentuan threshold 30 sebagai titik keseimbangan terbukti tepat karena berhasil menekan FAR hingga 0,00% baik pada tahap penentuan threshold maupun pada tahap evaluasi kinerja penuh, yang berarti sistem tidak pernah memberikan akses kepada pengguna yang tidak sah selama pengujian. Estimasi Equal Error Rate (EER) hasil interpolasi linier sebesar 0,83% menunjukkan titik temu yang sangat baik antara tingkat penerimaan palsu dan penolakan palsu. Kondisi ini menunjukkan bahwa sistem menekankan aspek keamanan, sesuai dengan kebutuhan sistem TTE yang harus memastikan bahwa proses penandatanganan elektronik hanya dilakukan

oleh pengguna yang sah berdasarkan regulasi yang berlaku [14].

Kenaikan nilai FRR dari 1,00% pada tahap penentuan threshold menjadi 12,73% pada evaluasi operasional skala penuh ($N = 450$) terbukti secara kuantitatif dipengaruhi oleh penurunan kualitas citra hasil akuisisi (skor NFIQ). Berdasarkan data empiris pada Tabel 4, sebanyak 76,19% kegagalan autentikasi (*False Negative*, $N = 42$) berasal dari sampel citra dengan NFIQ bernilai 4 dan 5. Citra berkategori buruk ini disebabkan oleh faktor teknis akuisisi di lapangan seperti kondisi permukaan kulit jari responden yang terlalu kering, terlalu lembap/berkeringat, serta variasi tekanan dan pergeseran posisi jari saat pemindaian. Ketersediaan minutiae yang sangat minim pada citra NFIQ 4–5 (< 15 titik minutiae) menyebabkan algoritma Bozorth3 tidak memiliki cukup pasangan geometris untuk menghasilkan skor pencocokan ≥ 30 . Temuan kuantitatif ini memperkuat analisis Dwivedi et al. (2023) dan Patel et al. (2022) mengenai sensitivitas algoritma Bozorth3 terhadap kualitas ekstraksi minutiae awal, sekaligus menegaskan perlunya penambahan modul *image enhancement* otomatis pada pra-pemrosesan citra untuk menekan FRR di masa depan [5].

Dari sisi efisiensi, total waktu autentikasi sebesar 0,30 detik menunjukkan bahwa sistem dapat diimplementasikan pada kebutuhan autentikasi real-time tanpa mengorbankan akurasi, sejalan dengan pandangan Kumar dan Singh (2023) bahwa sistem biometrik yang baik harus mampu bekerja cepat tanpa mengurangi tingkat akurasi [8]. Secara keseluruhan, penerapan autentikasi biometrik sidik jari pada sistem TTE terbukti memberikan lapisan keamanan tambahan yang lebih andal dibandingkan mekanisme konvensional berbasis username dan password [13], meskipun nilai FRR yang masih relatif tinggi menunjukkan perlunya perbaikan lanjutan pada tahap preprocessing citra untuk meningkatkan kenyamanan pengguna sah.

Pengujian alur transaksi TTE aktual pada Tabel 6 mengonfirmasi bahwa integrasi

biometrik NBIS tidak sekadar berfungsi sebagai modul verifikasi login terpisah sebagaimana pada Putra & Santoso (2024), melainkan terhubung secara langsung dengan mekanisme otorisasi pembentukan tanda tangan digital. Keberhasilan skenario pembatalan otomatis penandatanganan dokumen saat skor biometrik di bawah threshold 30 membuktikan bahwa sistem efektif mencegah akses penandatanganan tanpa hak. Dengan total waktu transaksi TTE sebesar 0,55 detik (termasuk verifikasi biometrik 0,30 detik dan pembuatan TTE 0,25 detik), sistem berhasil memenuhi tuntutan regulasi keamanan TTE (PP No. 71 Tahun 2019) dengan tetap memberikan performa yang responsif dan dapat diandalkan untuk operasional administrasi digital.

Dibandingkan dengan autentikasi konvensional berbasis *username/password* yang rentan terhadap *credential stuffing* dan penyalahgunaan identitas, penggunaan biometrik sidik jari memberikan perlindungan berbasis karakteristik fisik intrinsik yang tidak dapat dibagikan antar pengguna. Meskipun demikian, penelitian ini membatasi pengujian pada aspek performa statistik biometrik (*accuracy, FAR, FRR, processing time*) dan belum mencakup pengujian ketahanan terhadap serangan presentasi (*presentation attack/spoofing*) seperti penggunaan tiruan tiruan jari sintetis (*silicone/gelatin finger*). Pengujian *Liveness Detection* direkomendasikan sebagai pengembangan sistem selanjutnya untuk menguji keandalan fisik sistem terhadap *presentation attacks* secara langsung.

KESIMPULAN

Sistem autentikasi biometrik sidik jari berbasis metode minutiae-based matching dengan algoritma Bozorth3 telah berhasil dirancang dan diimplementasikan sebagai lapisan verifikasi identitas pada sistem Tanda Tangan Elektronik (TTE), mencakup seluruh tahapan mulai dari akuisisi citra, ekstraksi minutiae menggunakan MINDTCT, pembentukan template, hingga pencocokan

menggunakan Bozorth3. Berdasarkan pengujian terhadap 200 pasangan data genuine dan impostor, diperoleh threshold optimal sebesar 30 dengan FAR 0,00% dan FRR 1,00%. Evaluasi kinerja penuh terhadap 30 responden pada 450 percobaan autentikasi menghasilkan akurasi 90,67%, precision 100,00%, recall 87,27%, specificity 100,00%, FAR 0,00%, FRR 12,73%, serta rata-rata waktu autentikasi 0,30 detik. Hasil tersebut menunjukkan bahwa sistem mampu menolak seluruh pengguna tidak sah sekaligus bekerja secara efisien, sehingga menunjukkan potensi untuk digunakan sebagai mekanisme verifikasi identitas pada sistem TTE.

DAFTAR PUSTAKA

- [1] M. Ahmed, R. Hassan, and S. Ali, "Biometric authentication systems: Security and performance analysis," *International Journal of Information Security*, vol. 20, no. 4, pp. 455–468, 2021.
- [2] M. Al-Hussein and F. Alqahtani, "NBIS-based fingerprint verification for secure authentication systems," *Journal of Biometrics and Security*, vol. 18, no. 1, pp. 22–34, 2024.
- [3] A. Alshamrani, N. Alotaibi, and M. Alghamdi, "Performance evaluation of fingerprint matching algorithms in Linux-based biometric systems," *Computers & Security*, vol. 128, p. 103210, 2023.
- [4] Y. Chen, H. Wang, and X. Li, "Enhanced minutiae matching algorithm for fingerprint recognition under low-quality image conditions," *Pattern Recognition Letters*, vol. 158, pp. 45–53, 2022.
- [5] R. Dwivedi, P. Kumar, and S. Sharma, "Biometric integration for secure digital identity management," *Journal of Information Security and Applications*, vol. 72, p. 103432, 2023.
- [6] Information Technology—Biometric Performance Testing and Reporting—Part 1: Principles and Framework, ISO/IEC Standard 19795-1, 2021.

- [7] A. K. Jain, A. Ross, and K. Nandakumar, *Introduction to Biometrics and Fingerprint Recognition Systems*. New York: Springer, 2021.
- [8] V. Kumar and R. Singh, "Efficient fingerprint authentication on resource-constrained computing devices," *International Journal of Computer Applications*, vol. 185, no. 12, pp. 15–23, 2023.
- [9] M. Mahbub, M. Rahman, and A. Karim, "Minutiae-based fingerprint matching using NBIS framework," *International Journal of Biometrics*, vol. 14, no. 3, pp. 210–225, 2022.
- [10] National Institute of Standards and Technology, *NIST Biometric Image Software (NBIS) User's Guide*, NIST, Gaithersburg, MD, 2023.
- [11] T. Nguyen, H. Tran, and L. Pham, "Fingerprint authentication systems: Challenges and solutions," *Journal of Cyber Security Technology*, vol. 5, no. 4, pp. 245–260, 2021.
- [12] A. Nugroho, D. Pratama, and R. Santoso, "Strengthening electronic signature security through biometric authentication integration," *Indonesian Journal of Information Security*, vol. 11, no. 1, pp. 1–12, 2025.
- [13] R. Patel, M. Shah, and D. Mehta, "Security vulnerabilities in conventional authentication systems and biometric alternatives," *Information Security Journal*, vol. 31, no. 5, pp. 201–213, 2022.
- [14] Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, 2019.
- [15] A. Putra and B. Santoso, "Implementasi autentikasi biometrik sidik jari pada sistem tanda tangan elektronik berbasis NBIS," *Jurnal Rekayasa Sistem Informasi*, vol. 10, no. 1, pp. 55–66, 2024.
- [16] M. Rahman, S. Islam, and A. Karim, "Bozorth3 fingerprint matching performance evaluation in biometric authentication systems," *International Journal of Biometrics*, vol. 15, no. 2, pp. 101–118, 2023.
- [17] P. Sharma and R. Gupta, "Fingerprint recognition for secure authentication in digital systems," *International Journal of Computer Science and Security*, vol. 15, no. 2, pp. 90–102, 2021.
- [18] A. Wibowo and D. Pratama, "Analisis threshold optimal pada sistem autentikasi biometrik sidik jari menggunakan metode minutiae matching," *Jurnal Teknologi Informasi*, vol. 9, no. 2, pp. 112–123, 2024.
- [19] Y. Zhang and H. Liu, "Minutiae-based fingerprint matching with enhanced image normalization techniques," *Pattern Analysis and Applications*, vol. 23, no. 4, pp. 1551–1564, 2020.