

Digital Signature Implementation Using RSA and SHA-256 Algorithms for Authenticity Verification of Digital Certificate Images

Hezzekia Rafael Miracle¹, Christy Atika Sari^{2*}, Budi Handoko³

Teknik Informatika, Universitas Dian Nuswantoro

111202315281@mhs.dinus.ac.id¹, christy.atika.sari@dsn.dinus.ac.id^{2*}, handoko@dsn.dinus.ac.id³

Article Info

Article history:

Received 2026-08-11

Revised 2026-09-11

Accepted 2026-10-15

Keyword:

*Avalanche Effect,
Digital Signature,
RSA-2048,
SHA-256,
Verification certificate digital.*

ABSTRACT

The need for a system capable of accurately and rapidly verifying academic documents is crucial for ensuring the authenticity of digital certificates. This research implements a digital signature mechanism within the ECert Verify (Electronic Certificate Verification) system, utilizing the RSA-2048 algorithm alongside the PSS (Probabilistic Signature Scheme) padding scheme and the SHA-256 hash function to authenticate digital certificate images from Coursera. Each certificate is automatically converted into a 300 DPI (3508×2480 pixel) grayscale image to maintain hash consistency. The system was developed using Python with the pyca/cryptography library, Django for the backend, and React (Vite) for the frontend. Testing involved 20 datasets, comprising 5 authentic certificates and 15 manipulated samples (involving screenshots, re-compression, and content modification). Test results demonstrated a 100% verification accuracy rate, with no instances of false positives or false negatives. An average Avalanche Effect of 50.88% indicates that SHA-256 is highly sensitive to minor changes in the certificate image. Shannon Entropy testing yielded an average value of 7.1786 bits (89.73%)—close to the theoretical maximum of 8.0 bits—demonstrating a high level of randomness in the generated digital signatures. The average verification time was just 2.46 ms per file, indicating strong performance in a controlled single-user testing environment. Furthermore, a limited user acceptance survey regarding the interface's operational aspects revealed that the system is highly rated and functional in supporting the certificate issuance process for operators.



This is an open access article under the [CC-BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.

I. PENDAHULUAN

Perkembangan yang cepat dalam bidang teknologi informasi telah menyebabkan terjadinya digitalisasi di berbagai sektor, salah satunya terjadi di sektor pendidikan dan sertifikasi yang kini semakin canggih dan berkembang [1]. Perubahan yang paling terlihat adalah dengan beralihnya pengolahan dokumen akademik ke sistem elektronik, khususnya yang paling banyak digunakan saat ini adalah sertifikat digital [2]. Perubahan ini tidak hanya untuk keperluan efisiensi operasional, tetapi juga untuk mendapatkan akses data yang lebih cepat dan fleksibel dalam era digital sekarang ini [3]. Pada praktiknya, dokumen berbasis elektronik telah menjadi acuan utama dalam sistem administrasi pendidikan maupun platform pembelajaran

daring guna mendukung integrasi sistem informasi yang lebih optimal [4].

Di mata hukum, sertifikat digital memiliki kedudukan yang sah sebagai dokumen elektronik dengan kekuatan hukum dan konsekuensi yang signifikan [5]. Dalam konteks akademik, sertifikat digital memiliki peran sebagai alat validasi atas capaian atau kelulusan seorang individu, meskipun dalam pengelolaannya masih rentan terhadap pemalsuan dan penyalahgunaan dokumen [6], [7]. Laporan penelitian lain mengidentifikasi bahwa permasalahan sertifikat palsu telah menjadi isu global, salah satunya di Amerika Serikat ditemukan sekitar 2 juta sertifikat palsu yang beredar, yang membuktikan besarnya risiko manipulasi data jika tidak disertai sistem keamanan atau mekanisme verifikasi yang memadai [8], [9]. Risiko ini menjadi semakin serius mengingat sertifikat digital merupakan salah satu persyaratan

utama dalam berbagai kebutuhan administratif, mulai dari proses rekrutmen kerja hingga akses ke jenjang pendidikan yang lebih tinggi [10]. Oleh sebab itu, institusi penerbit dituntut untuk menjamin sepenuhnya keutuhan data serta keaslian informasi yang tercantum di dalamnya [11].

Tuntutan tersebut mendorong munculnya berbagai upaya untuk mengatasi pemalsuan yang semakin mudah dilakukan dengan teknologi penyuntingan citra digital, sehingga diperlukan sistem yang mampu memverifikasi keaslian dokumen sertifikat secara efisien, akurat, dan aman [12], [13]. Beberapa penelitian sebelumnya telah mengusulkan berbagai metode pengamanan, mulai dari penggunaan kode unik hingga pemanfaatan teknologi buku besar terdistribusi untuk menjaga validitas data dokumen dari perubahan yang tidak sah [14], [15], [16]. Namun, fokus utama tetap terletak pada bagaimana memastikan bahwa file citra yang dipegang pengguna tetap identik dengan data aslinya [17].

Penelitian terdahulu secara khusus menguji efektivitas digital signature dalam menjaga integritas dokumen digital. Satyaldy dkk. [15] menegaskan bahwa proses verifikasi autentisitas melalui skema digital dapat diselesaikan dalam hitungan detik, yang secara teknis menjamin dokumen bersifat tahan manipulasi (*tamper-proof*). Ini sejalan dengan temuan Kontzinos dkk. [14] yang melakukan uji coba platform berbasis desentralisasi, di mana proses verifikasi konvensional yang biasanya memakan waktu hingga satu minggu, dapat dipangkas secara signifikan menjadi hanya sekitar 1,3 detik dengan efisiensi biaya operasional yang optimal.

Selain aspek keamanan, efisiensi waktu verifikasi menjadi parameter keberhasilan sebuah sistem verifikasi sertifikat. Baniata dkk. [16] memberikan landasan teknis mengenai pemilihan algoritma kriptografi, di mana dalam pengujian mereka, algoritma berbasis asimetris menunjukkan performa verifikasi yang sangat cepat, dengan rentang waktu berada pada kisaran 0,003 hingga mencapai sekitar 0,14 detik. Keunggulan performa verifikasi ini menjadi alasan kuat dalam pemilihan metode kriptografi asimetris untuk menangani validasi sertifikat dalam skala luas. Akan tetapi, sebagian besar penelitian terdahulu [14]-[16] lebih berfokus pada pembangunan infrastruktur jaringan terdistribusi dan blockchain yang kompleks untuk mengolah data teks terstruktur (*metadata/JSON*). Hal ini menimbulkan gap penelitian di mana peneliti terdahulu belum menerapkan tahap standarisasi prapemrosesan citra digital, sehingga sistem verifikasi rentan gagal membedakan berkas asli dari berbagai teknik manipulasi visual seperti *screenshot*, kompresi ulang, maupun penyunting konten. Meskipun banyak penelitian menggunakan platform blockchain, prinsip utama yang ditekankan adalah bagaimana menjaga validitas data dari perubahan yang tidak sah melalui enkripsi dan hashing [18].

Berdasarkan tinjauan dan keterbatasan penelitian terdahulu tersebut, penelitian ini menerapkan mekanisme Digital

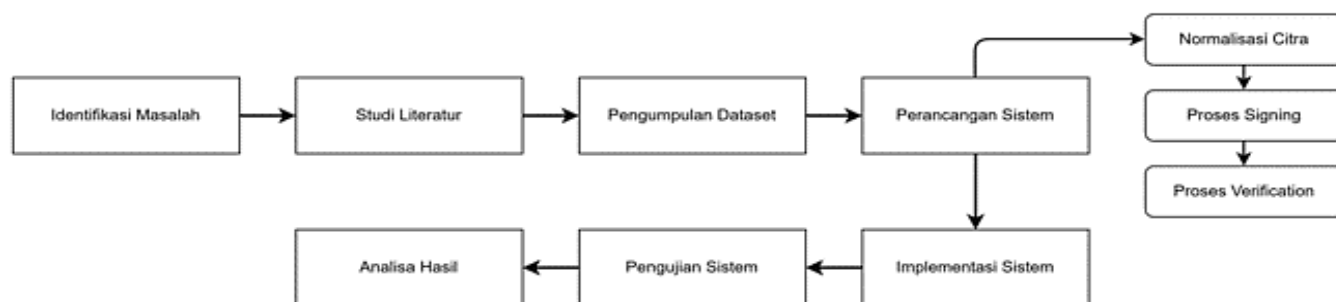
Signature pada citra sertifikat digital untuk memastikan keaslian dan mendeteksi perubahan dokumen secara otomatis. Sistem yang dikembangkan diberi nama ECert Verify (*Electronic Certificate Verification*), sebuah sistem verifikasi keaslian sertifikat digital berbasis web yang bekerja dengan prinsip registrasi terlebih dahulu. Penerbit sertifikat mendaftarkan dokumen asli melalui proses *signing* menggunakan Private Key, kemudian pihak validator dapat mengecek keaslian dokumen tersebut menggunakan Public Key dan Digital Signature yang dihasilkan. Berbeda dengan penelitian sebelumnya yang berfokus pada infrastruktur jaringan terdistribusi, penelitian ini menitikberatkan pada keandalan algoritma RSA-2048 dengan skema padding PSS (*Probabilistic Signature Scheme*) dan fungsi hash SHA-256 [19]. Pemilihan algoritma RSA-2048 dengan skema padding PSS didasarkan pada kematangan implementasi, dukungan library kriptografi yang luas, serta kompatibilitas dengan standar industri yang telah terbukti [19]. Perbandingan performa dan keamanan antara RSA-2048 PSS dengan algoritma digital signature alternatif seperti *Elliptic Curve Digital Signature Algorithm (ECDSA)* merupakan arah pengembangan yang direkomendasikan untuk penelitian selanjutnya guna menentukan *trade-off optimal* antara ukuran kunci, kecepatan komputasi, dan tingkat keamanan.

Kontribusi utama dan kebaruan (*novelty*) dari penelitian ini terletak pada arsitektur integrasi fungsional antara skema *image pre-processing pipeline* otomatis dengan mekanisme kriptografi asimetris tersebut. Keunikan sistem ECert Verify terletak pada proses normalisasi citra ke format *grayscale 300 DPI* sebelum proses hashing dilakukan, guna memastikan konsistensi nilai data [20]. Pemilihan citra digital (*certificate image*) sebagai objek yang ditandatangani didasarkan pada pertimbangan bahwa verifikasi sertifikat dalam praktiknya dilakukan secara visual oleh pihak penerima. Pendekatan ini sekaligus berfungsi sebagai *proof-of-concept* untuk menguji efektivitas normalisasi citra dalam menjaga konsistensi nilai hash, yang menjadi fondasi utama sistem verifikasi ini. Dengan menerapkan tanda tangan digital langsung pada tingkat piksel citra terstandar, sistem ini menjamin integritas visual dokumen dapat diverifikasi secara mandiri. Kekuatan kriptografi yang dihasilkan kemudian diuji secara empiris menggunakan metode *Shannon Entropy* dan *Avalanche Effect* untuk membuktikan ketahanan sistem terhadap upaya manipulasi data.

II. METODE

A. Tahap Penelitian

Penelitian ini dilaksanakan melalui serangkaian tahapan yang sistematis guna memastikan pengembangan sistem verifikasi sertifikat digital berjalan secara terarah. Tahapan tersebut ditunjukkan pada Gambar 1.



Gambar 1. Tahapan penelitian

Penjelasan detail tiap tahapan pada Gambar 1 adalah sebagai berikut:

1. Identifikasi Masalah

Tahap awal adalah menganalisa kerentanan manipulasi pada citra sertifikat digital dan kebutuhan akan sistem deteksi otomatis yang mampu menjamin integritas data tanpa bergantung pada pihak ketiga secara terus-menerus.

2. Studi Literatur

Mempelajari teori dan penelitian terdahulu mengenai algoritma RSA-2048, skema padding PSS, fungsi hash SHA-256, serta teknik pengolahan citra digital untuk menunjang keamanan informasi.

3. Pengumpulan Dataset

Dataset yang digunakan dalam penelitian ini adalah e-sertifikat dari platform belajar online Coursera yang merupakan milik peneliti sendiri, yang dikonversi menjadi citra digital grayscale 300 DPI guna menjamin konsistensi nilai hash SHA-256. Pada tahap ini, dataset tersebut dibagi menjadi dua jenis kategori pengujian, yaitu: (1) e-sertifikat asli yang tidak dimodifikasi dan berfungsi sebagai ground truth setelah proses signing, dan (2) versi yang telah dimanipulasi atau tampered dari e-sertifikat asli. Proses rekayasa data tampered dilakukan dengan tiga pendekatan, yaitu screenshots layar sertifikat, kompresi ulang file PDF, dan modifikasi isi teks (nama, tanggal terbit, atau judul kursus) dengan editor gambar. Jumlah total data yang telah dikumpulkan dan disiapkan dalam tahap ini sebanyak 20 data, yang terdiri dari 5 sertifikat asli dan 15 versi manipulasi.

4. Perancangan Sistem

Perancangan arsitektur sistem secara mendalam mencakup tiga sub-proses utama:

- **Normalisasi Citra:** Proses menyamakan format, resolusi (300 DPI), dan warna (grayscale) citra untuk memastikan nilai hashing yang konsisten.
- **Proses Signing:** Perancangan alur pembuatan tanda tangan digital menggunakan algoritma RSA-2048 dengan skema padding PSS (Probabilistic Signature Scheme) dan fungsi hash SHA-256.

- **Proses Verification:** Perancangan mekanisme validasi sertifikat menggunakan kunci public untuk membandingkan nilai hash asli dengan hash pada dokumen yang dipegang pengguna.

5. Implementasi Sistem

Mengimplementasikan rancangan ke dalam kode program menggunakan Python dengan library kriptografi pyca/cryptography, Django dan Django REST Framework sebagai backend, serta React (Vite) sebagai frontend untuk membangun sistem verifikasi sertifikat digital yang fungsional.

6. Pengujian Sistem

Melakukan pengujian terhadap kemampuan sistem dalam mendeteksi perubahan sekecil apapun (manipulasi piksel) pada citra sertifikat. Seluruh pengujian dilaksanakan pada lingkungan eksperimen dengan spesifikasi perangkat keras sebagai berikut: prosesor AMD Ryzen 7 5800H dengan kecepatan 3,20 GHz, memori RAM sebesar 24 GB, serta sistem operasi Windows 11 Home (64-bit). Pengukuran waktu eksekusi mencakup keseluruhan proses pada setiap tahapan, mulai dari normalisasi citra, hashing SHA-256, signing RSA-2048 PSS, hingga verifikasi signature, sebagaimana dirinci pada Tabel V.

7. Analisa Hasil

Melakukan evaluasi terhadap kekuatan kriptografi menggunakan metode empiris seperti Avalanche Effect untuk mengukur sensitivitas algoritma dan Shannon Entropy untuk menganalisis keacakan data.

Sebagai dasar teori dalam tahap perancangan sistem, cara pembuatan kunci dalam algoritma asimetris RSA (Rivest-Shamir-Adleman) didasarkan pada penggunaan fungsi satu arah dengan pintu rahasia (trapdoor one-way function) yang memanfaatkan kompleksitas dalam memfaktorkan dua bilangan prima yang besar. Secara matematis, proses pembuatan kunci yang efektif berlangsung melalui rumus berikut [21]:

1. Pilih dua bilangan prima acak rahasia berukuran besar, p dan q .
2. Hitung nilai modulus n dengan persamaan (1).

$$n = p \times q \quad (1)$$

3. Hitung fungsi totien Euler menggunakan persamaan (2).

$$\phi(n) = (p - 1)(q - 1) \quad (2)$$

4. Pilih kunci public e secara acak dengan syarat e harus koprima dengan $\phi(n)$ dan memenuhi batasan $1 < e < \phi(n)$.
5. Hitung kunci privat d melalui penyelesaian invers perkalian modular pada persamaan (3).

$$e \cdot d \equiv 1 \pmod{\phi(n)} \quad (3)$$

Pasangan kunci public (e, n) dan kunci privat (d, n) yang dihasilkan dari landasan matematis ini selanjutnya akan didistribusikan ke dalam sistem ECert Verify untuk memproses pengamanan dokumen, di mana implementasi operasional dari proses signing dan verifikasi secara spesifik dijabarkan pada Bab III.

B. Dataset Penelitian

Dataset yang digunakan dalam penelitian ini merupakan e-sertifikat dari platform pembelajaran daring Coursera yang merupakan milik peneliti sendiri. E-sertifikat dari platform Coursera secara default diterbitkan dalam format PDF sebagai format distribusi resminya. Oleh karena itu, sebelum diproses oleh sistem, setiap file PDF dikonversi secara otomatis oleh sistem ECert Verify menjadi citra digital (digital image) dalam format grayscale dengan resolusi 300 DPI (3508×2480 piksel), sehingga objek yang diproses dan diverifikasi oleh sistem adalah citra digital dari sertifikat tersebut, bukan file PDF nya secara langsung.

Proses normalisasi citra ke format grayscale 300 DPI digunakan untuk memastikan bahwa nilai hash SHA-256 yang dihasilkan bersifat konsisten untuk setiap file yang identik, terlepas dari platform atau perangkat yang digunakan untuk mengakses sertifikat. Penggunaan sertifikat digital yang dipilih merupakan sertifikat digital asli milik peneliti sendiri, guna merepresentasikan kondisi penggunaan sistem verifikasi pada skenario nyata, sekaligus menghindari permasalahan privasi yang berkaitan dengan penggunaan dokumen milik pihak lain.

Berdasarkan Tabel 1, total keseluruhan data pengujian yang digunakan berjumlah 20 data, terdiri dari 5 sertifikat asli sebagai kategori original dan 15 variasi manipulasi sebagai kategori tampered yang dibagi rata ke dalam tiga jenis manipulasi. Pemilihan tiga jenis manipulasi tersebut didasarkan pada skenario pemalsuan yang paling umum terjadi di lapangan, mulai dari pemalsuan sederhana seperti screenshot hingga pemalsuan konten yang lebih berbahaya seperti modifikasi nama pemegang dan tanggal terbit sertifikat. Secara lebih rinci, parameter teknis pada skenario manipulasi dirancang untuk mensimulasikan metode pemalsuan dokumen yang paling sering terjadi di lingkungan Masyarakat umum menggunakan peralatan berbasis web

(web-based tools). Pada skenario screenshot, dokumen ditangkap langsung menggunakan fitur standar sistem operasi (Print Screen) untuk menguji ketahanan sistem terhadap hilangnya struktur biner asli berkas PDF akibat konversi otomatis menjadi format gambar 24-bit RGB. Pada skenario kompresi ulang, file diproses menggunakan web-based PDF compressor gratis yang menerapkan algoritma kompresi berbasis blok (lossy compression), yang secara otomatis memangkas ukuran biner dokumen asli. Sementara itu, pada skenario modifikasi konten, manipulasi dilakukan melalui platform online PDF editor untuk mengubah string teks krusial, seperti nama pemegang sertifikat dan tanggal terbit, memanfaatkan fitur pencocokan jenis huruf (font matching) otomatis yang disediakan oleh platform tersebut. Pengujian terhadap manipulasi tingkat piksel seperti perubahan brightness, rotation, atau resize merupakan arah pengembangan yang direkomendasikan untuk penelitian selanjutnya.

TABEL I

DISTRIBUSI DATASET PENGUJIAN

No	Kategori	Jumlah	Keterangan
1	Original	5 file	E-sertifikat Coursera asli format PDF resmi.
2	Tampered – Screenshot	5 variasi	Fitur bawaan sistem operasi (Print Screen / PrtSc), format gambar PNG/JPEG, kedalaman warna 24-bit RGB
3	Tampered – Kompresi ulang	5 variasi	Web-based PDF compressor (IlovePDF/Smallpdf), reduksi ukuran berkas otomatis via kompresi berbasis blok (lossy).
4	Tampered – Modifikasi Konten	5 variasi	Web-based PDF Editor (Sejda/PDFCandy), pemalsuan string teks pada nama dan tanggal dengan pencocokan font otomatis.

Pada Gambar 2 ditunjukkan perbandingan antara sertifikat Coursera dalam kondisi asli dan hasil normalisasi citra oleh sistem ECert Verify ditunjukkan. Proses normalisasi ini dilakukan secara otomatis oleh sistem setiap kali sertifikat diunggah, sehingga peneliti tidak perlu melakukan konversi secara manual sebelum pengujian dilakukan. Pada Gambar 2, (a) sertifikat Coursera dalam kondisi asli yang masih mempertahankan warna dan format PDF originalnya, sedangkan (b) merupakan hasil konversi otomatis oleh sistem ECert Verify ke format grayscale dengan resolusi 300 DPI (3508×2480 piksel), yang akan digunakan sebagai input proses hashing SHA-256. Perbedaan yang terlihat secara visual antara keduanya menunjukkan bahwa sistem berhasil melakukan normalisasi citra sebelum proses hashing SHA-256 dilakukan. Meskipun tampilannya berubah menjadi grayscale, seluruh informasi penting pada sertifikat seperti nama pemegang, judul kursus, tanggal terbit, dan tanda

tangan tetap terbaca jelas, ini membuktikan bahwa proses normalisasi tidak merusak integritas konten dokumen.

Ketetapan resolusi 300 DPI dengan dimensi absolut 3508×2480 piksel ini merupakan ambang batas normalisasi mutlak (forced normalization) yang dirancang untuk mengatasi sifat sensitif dari fungsi hash SHA-256. Karakteristik utama dari fungsi hash kriptografi adalah adanya efek domino (avalanche effect), di mana perubahan sekecil satu bit atau satu piksel pada input akan merombak nilai digest secara radikal. Dalam praktiknya, manipulasi geometri berupa pengubahan ukuran (resizing), pemotongan (cropping), atau variasi format kompresi citra merekonstruksi ulang susunan matriks biner berkas gambar. Melalui penetapan matriks acuan baku (anchor matrix) berbasis ukuran cetak standar kertas A4 (300 DPI), setiap dokumen yang diunggah akan dipaksa menuju struktur piksel yang identik.

Selain penyeragaman geometri, konversi ke format grayscale (1 channel warna) juga krusial untuk mengeliminasi gangguan variasi informasi warna (color noise atau chrominance channels) dari berkas PDF asli yang rentan mengalami pergeseran nilai biner saat proses rasterisasi. Dengan mereduksi representasi data dari RGB (3 channels) menjadi grayscale, sistem mampu mempertahankan ketajaman spasial elemen tekstual halus sekaligus mengunci konsistensi nilai hash piksel. Skema ini memastikan bahwa verifikasi integritas dokumen bertumpu sepenuhnya pada keaslian informasi visual yang tertera pada sertifikat, bukan pada atribut meta-data atau variasi rendering warna di latar belakang.

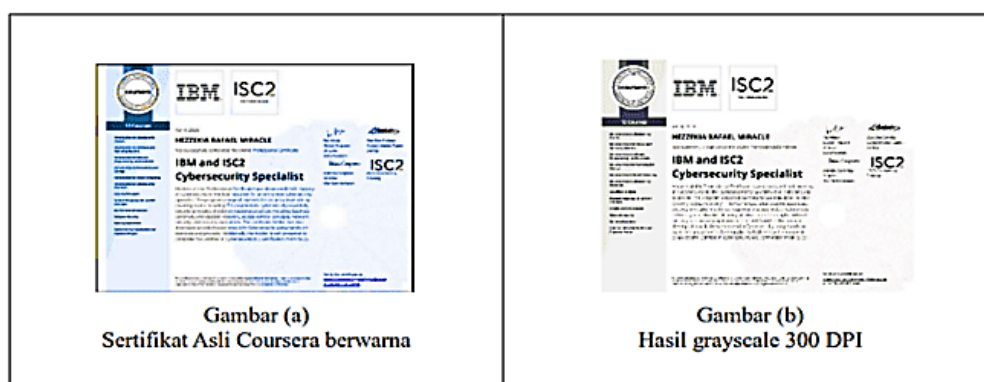
Dari perspektif kriptografi, rekonstruksi citra melalui tahapan forced normalization ini secara spesifik dirancang untuk mengejar konsistensi pada tingkat biner (byte-level consistency), bukan sekadar kemiripan visual (visual consistency) yang ditangkap oleh indra penglihatan manusia. Algoritma SHA-256 bekerja secara ketat pada representasi

aliran bit (bitstream) dokumen. Akibatnya, dua buah citra sertifikat yang tampak kembar identik secara visual tetap akan menghasilkan nilai hash yang berbeda jika terdapat variasi pada struktur internal berkasnya. Perbedaan laten ini umumnya dapat dipicu oleh variasi perangkat, platform rendering, atau artefak akibat algoritma kompresi data pada format tertentu.

Untuk mengatasi inkonsistensi tersebut, sistem secara otomatis membuang seluruh informasi metadana bawaan serta mengunci output normalisasi ke dalam format PNG yang bersifat lossless compression, sistem memaksa penyelarasan susunan byte (byte-level alignment) secara absolut. Pendekatan ini menjamin bahwa setiap sertifikat dengan konten visual yang sama akan selalu direpresentasikan oleh rangkaian byte yang identik, sehingga menghasilkan nilai hash SHA-256 yang konsisten dan valid.

Pendekatan normalisasi ini juga memberikan ketahanan terhadap perubahan format yang tidak disengaja, karena mekanisme konversi grayscale dan standardisasi resolusi LANCZOS bersifat deterministik sehingga perubahan non-visual seperti modifikasi metadana EXIF atau re-save tanpa kompresi lossy tidak akan mempengaruhi nilai hash yang dihasilkan. Namun, sistem ini memiliki keterbatasan terhadap perubahan piksel akibat kompresi lossy di luar pipeline sistem, misalnya melalui platform berbagi file yang secara otomatis mengompresi ulang file. Kondisi ini diakui sebagai keterbatasan yang dapat diatasi pada penelitian selanjutnya dengan menerapkan perceptual hashing sebagai lapisan tambahan.

Untuk ukuran berkas PDF sertifikat asli yang digunakan memiliki rentang ukuran berkas antara 281 KB hingga 386 KB (dengan rata-rata 315,8 KB). Setelah dikonversi secara otomatis oleh sistem ECert Verify menjadi citra digital grayscale 300 DPI berformat PNG, berkas citra yang dihasilkan berada pada kisaran ukuran 837 KB hingga 1.217 KB (dengan rata-rata sebesar 922,4 KB).



Gambar 2. Visualisasi normalisasi citra sertifikat digital: (a) sertifikat asli Coursera dalam format PDF berwarna, (b) hasil konversi sistem ECert Verify ke format grayscale 300 DPI (3508×2480 piksel)

C. Arsitektur Sistem

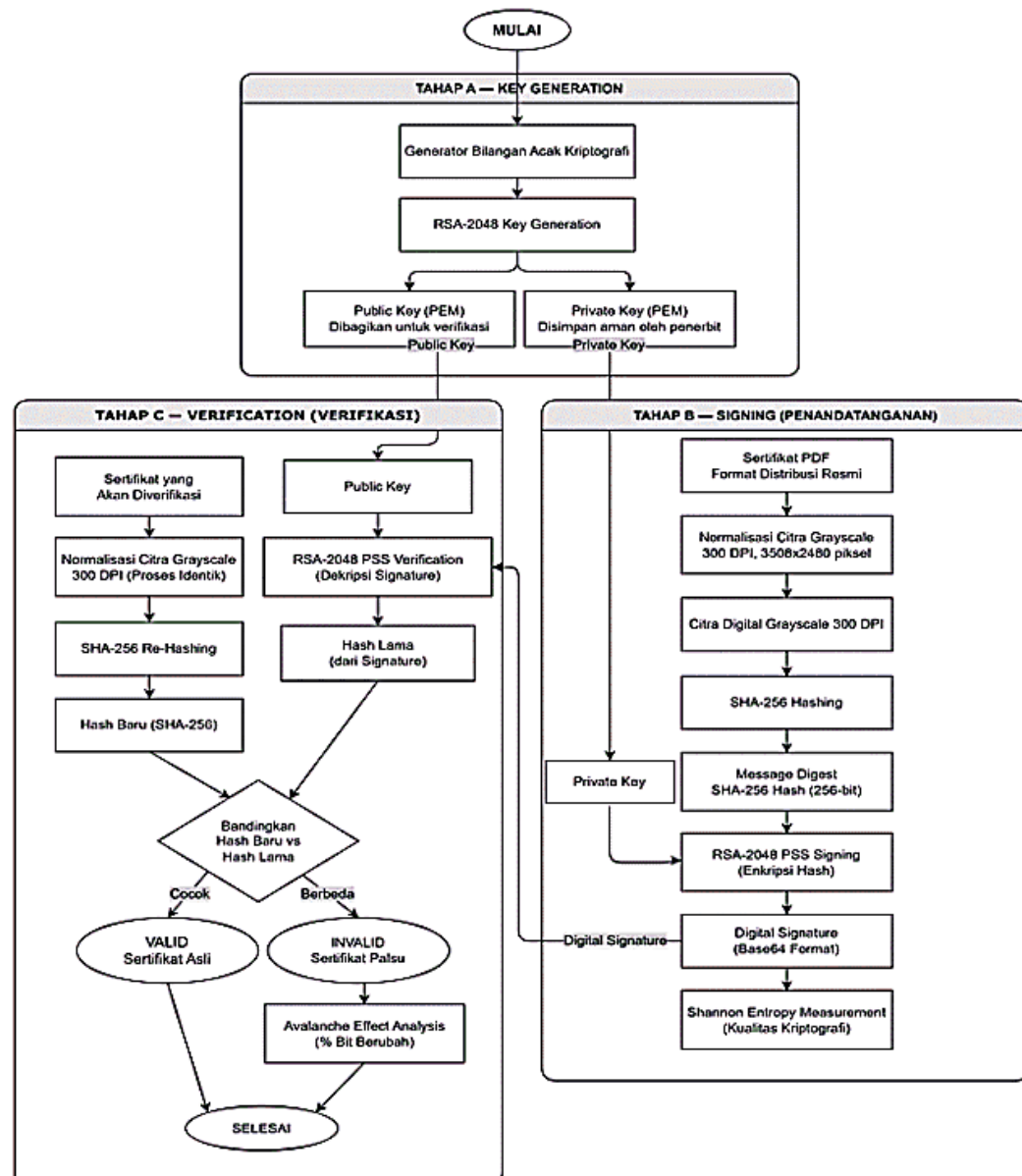
Arsitektur sistem yang dirancang terdiri dari tiga tahapan utama yang saling terintegrasi untuk menjamin keamanan dan

otentisitas sertifikat digital, yaitu tahapan Key Generation, Signing, dan Verification. Detail alur kerja sistem secara

lengkap, mulai dari proses pembangkitan kunci hingga verifikasi keaslian sertifikat, ditunjukkan pada Gambar 3.

Berdasarkan Gambar 3, alur perancangan sistem verifikasi sertifikat digital terbagi menjadi tiga tahapan utama yang saling terhubung. Tahap pertama adalah pembangkitan kunci, dua kunci RSA-2048 (private key dan public key) dihasilkan melalui generator bilangan acak kriptografi, ini digunakan untuk menjamin keamanan asimetris. Tahap kedua adalah proses penandatanganan digital, di mana citra sertifikat yang

telah melalui proses normalisasi (grayscale 300 DPI) diproses menggunakan fungsi SHA-256 untuk menghasilkan message digest, yang kemudian dienkripsi dengan private key menggunakan skema RSA-2048 PSS. Tahap terakhir adalah verifikasi, sistem membandingkan nilai hash baru dari berkas citra dengan hasil dekripsi tanda tangan digital menggunakan public key, jika kedua nilai identik maka sertifikat dinyatakan valid, jika tidak sistem akan melakukan analisis Avalanche Effect untuk mendeteksi tingkat manipulasi pada data.



Gambar 3. Alur Perancangan Sistem

Berdasarkan rancangan tersebut, mekanisme manajemen tanda tangan digital (digital signature) pada sistem ini secara spesifik mengadopsi pendekatan detached signature (tanda tangan terlepas). Nilai tanda tangan digital yang dihasilkan

dari enkripsi pesan digest SHA-256 menggunakan kunci privat RSA-2048 dilepaskan sebagai entitas independent dalam format string Base64 yang berada di luar berkas citra maupun pangkalan data server. Karakteristik arsitektur yang

bersifat stateless ini ditunjukkan secara eksplisit pada diagram alur TAHAP C (VERIFICATION) pada Gambar 3. Pada tahap tersebut, string tanda tangan digital bertindak sebagai komponen masukan (input) eksternal terpisah yang wajib diserahkan kembali oleh pihak penerbit sertifikat secara bersamaan dengan berkas sertifikat dan kunci publik (public key). Melalui pemisahan alur penandatanganan dan verifikasi ini, sistem mampu membuktikan otentisitas dokumen dengan memanfaatkan komputasi matematis murni dari skema RSA-2048 PSS tanpa memiliki ketergantungan pada penyimpanan internal server. Pendekatan desain ini sengaja dipilih guna mengeliminasi beban penyimpanan pada basis data serta memfokuskan pengujian performa kriptografi pada analisis avalanche effect dan Shannon entropy.

Perlu dicatat bahwa tanggung jawab penyimpanan berkas tanda tangan digital sepenuhnya berada pada pihak penerbit sertifikat sebagai operator sistem. Kegagalan dalam pengelolaan berkas signature oleh penerbit akan mengakibatkan proses verifikasi tidak dapat dilakukan, sehingga diperlukan prosedur manajemen berkas yang ketat di sisi institusi penerbit. Hal ini merupakan konsekuensi yang disengaja dari pendekatan stateless, sebagai trade-off untuk menghindari ketergantungan pada infrastruktur penyimpanan terpusat

D. Parameter Pengujian

Performa sistem digital signature RSA-2048 dan SHA-256 diuji menggunakan dua parameter utama untuk mengukur tingkat keamanan dan sensitivitas deteksi manipulasi. Parameter Avalanche Effect digunakan untuk mengukur sejauh mana perubahan kecil pada citra sertifikat (seperti modifikasi satu piksel) dapat menghasilkan perubahan signifikan pada nilai hash dan tanda tangan digital yang dihasilkan. Selain itu, pengujian Shannon Entropy dilakukan untuk mengetahui tingkat keacakan informasi pada tanda tangan digital guna memastikan ketahanan terhadap upaya analisis pola oleh pihak yang tidak berwenang. Dengan kedua parameter tersebut, keberhasilan algoritma dalam mempertahankan integritas dan autentisitas citra sertifikat dapat dianalisis secara menyeluruh. Avalanche Effect dan Shannon Entropy dalam penelitian ini secara spesifik diposisikan bukan sebagai indikator utama keamanan skema RSA-PSS secara kriptografis, melainkan sebagai metrik empiris untuk memvalidasi kualitas fungsi hash SHA-256 sebagai komponen fondasi sistem. Avalanche Effect membuktikan bahwa SHA-256 bereaksi secara deterministik dan sensitif terhadap setiap perubahan pada citra sertifikat, sementara Shannon Entropy yang diukur terhadap distribusi bit-level dari string Base64 tanda tangan digital yang dihasilkan membuktikan bahwa output sistem tidak mengandung pola statistik yang dapat dieksploitasi. Kedua metrik ini dipilih karena relevansinya dalam mengkuantifikasi ketahanan sistem terhadap manipulasi visual pada tingkat piksel, yang merupakan fokus utama penelitian ini.

III. HASIL DAN PEMBAHASAN

A. Analisis Algoritma RSA dan SHA-256

Pengamanan citra digital dalam penelitian ini menggunakan mekanisme digital signature yang menggabungkan kekuatan algoritma asimetris RSA dengan fungsi hash kriptografi SHA-256. Algoritma RSA-2048 menjadi komponen utama dalam proses penandatanganan dan verifikasi tanda tangan digital, sedangkan SHA-256 digunakan untuk menghasilkan nilai hash yang merepresentasikan integritas citra sertifikat secara unik. Dalam penelitian ini, objek yang diproses bukan lagi pesan teks biasa, melainkan representasi digital dari citra sertifikat yang telah diekstraksi nilai hash-nya. Oleh karena itu, hubungan fungsional antara proses signing dan verifikasi pada sistem ECert Verify disesuaikan menggunakan nilai hash SHA-256 pada proses signing sesuai persamaan (4) dan proses verifikasi sesuai persamaan (5).

$$S = H(P)^d \bmod n \quad (4)$$

$$H' = S^e \bmod n \quad (5)$$

Di mana:

- S adalah digital signature yang dihasilkan dari citra sertifikat
- $H(P)$ adalah nilai hash 256-bit yang dihasilkan dari representasi piksel citra (P) dalam format grayscale 300 DPI menggunakan fungsi SHA-256.
- H' adalah nilai hash hasil dekripsi signature yang akan dibandingkan dengan hash citra yang baru dihitung.
- d dan e merupakan komponen kunci asimetris yang menjamin autentisitas pengirim.

Keunggulan penggunaan RSA-2048 dengan skema padding PSS (*Probabilistic Signature Scheme*) terletak pada sifat probabilistiknya yang menghasilkan nilai signature berbeda untuk setiap sesi penandatanganan meskipun dengan pesan yang sama. Sementara itu, SHA-256 menjamin sifat collision resistance dan pre-image resistance yang tinggi. Kekuatan kriptografi yang dihasilkan kemudian diuji secara empiris menggunakan metode Shannon Entropy dan Avalanche Effect untuk membuktikan ketahanan sistem terhadap upaya manipulasi data

B. Parameter Pengujian

Untuk mengetahui seberapa baik dan andal sistem digital signature berbasis RSA-2048 dan SHA-256 yang telah dibangun, dilakukan pengujian dengan menggunakan tiga parameter metrik penilaian. Shannon Entropy digunakan untuk mengukur derajat keacakan pada nilai hash SHA-256 yang dihasilkan. Nilai entropy yang mendekati 8 menunjukkan bahwa distribusi bit hash memiliki ketahanan statistik yang baik terhadap analisis kriptografi sesuai persamaan (6).

$$H(m) = - \sum_{i=0}^{255} P(m_i) \log_2 P(m_i) \quad (6)$$

Avalanche Effect digunakan untuk mengukur sensitivitas fungsi hash SHA-256 terhadap perubahan kecil pada citra sertifikat. Nilai avalanche effect yang ideal mendekati 50%, menandakan bahwa perubahan satu bit pada masukan menghasilkan perubahan sekitar setengah dari seluruh bit keluaran hash sesuai persamaan (7).

$$AE = \left(\frac{\text{Jumlah bit berbeda}}{\text{Total bit hash}} \right) \times 100\% \quad (7)$$

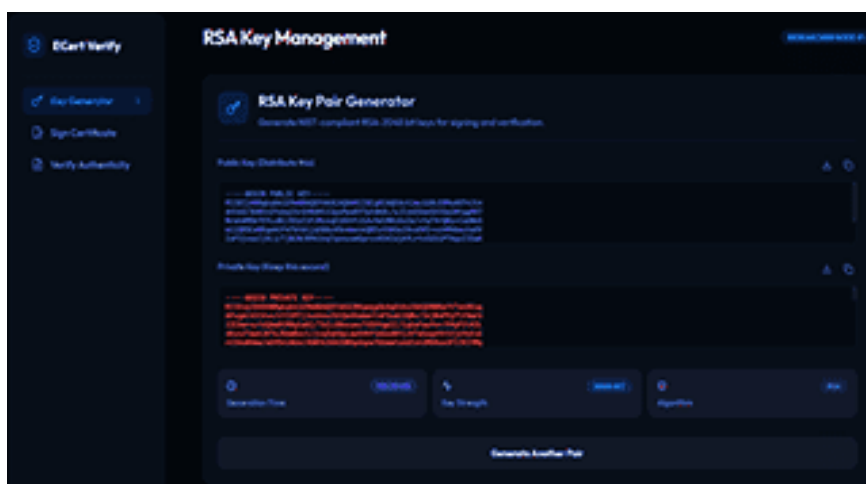
Waktu Eksekusi (Execution Time) digunakan untuk mengukur efisiensi kinerja sistem ECert Verify dalam proses *signing* dan verifikasi. Pengukuran dilakukan dalam satuan milidetik (ms) dengan mencatat selisih waktu antara awal dan akhir proses sesuai persamaan (8).

$$T = T_{end} - T_{start} \quad (8)$$

Ketiga parameter tersebut diuji secara empiris menggunakan sejumlah sampel citra sertifikat digital dalam format grayscale 300 DPI. Pengujian Shannon Entropy dan Avalanche Effect bertujuan untuk membuktikan kekuatan kriptografi sistem, sementara pengukuran waktu eksekusi digunakan untuk menilai kelayakan sistem dalam penerapan nyata. Seluruh pengujian dilakukan pada lingkungan yang terkontrol untuk memastikan konsistensi dan validitas hasil yang diperoleh.

C. Hasil Implementasi dan Analisis

Sistem dibangun menggunakan bahasa pemrograman Python dan library kriptografi *pyca/cryptography*, Django dan Django REST Framework sebagai backend, serta React (Vite) sebagai frontend. Sistem terdiri dari tiga menu utama, yaitu Key Generator, Sign Certificate, dan Verify Authenticity, yang masing-masing menangani tahapan proses yang berbeda. Tampilan menu Key Generator ditunjukkan pada Gambar 4.



Gambar 4. Tampilan Menu Key Generator yang menampilkan Public Key dan Private Key RSA-2048

Berdasarkan Gambar 4, menu Key Generator menampilkan pasangan kunci RSA-2048 yang dihasilkan secara otomatis oleh sistem melalui generator bilangan acak kriptografi standar NIST. Public Key ditampilkan pada bagian atas dan dapat didistribusikan kepada pihak validator yang memerlukan hak akses verifikasi, sedangkan Private Key ditampilkan pada bagian bawah dan wajib disimpan secara aman oleh penerbit sertifikat. Kedua Key tersebut dilengkapi fitur unduh langsung berformat .pem untuk memudahkan penggunaannya. Pada metrik performa, sistem mencatatkan waktu Generation Time sebesar 103,30 ms untuk membentuk kekuatan kunci (Key Strength) 2048-bit menggunakan algoritma RSA. Seperti yang ditampilkan pada Tabel 5, nilai waktu eksekusi riil ini bersifat dinamis karena

dipengaruhi oleh kondisi alokasi memori dan beban kerja prosesor komputer sesaat pada sesi pengujian tersebut. Berikutnya Gambar 5 menampilkan menu Sign Certificate.

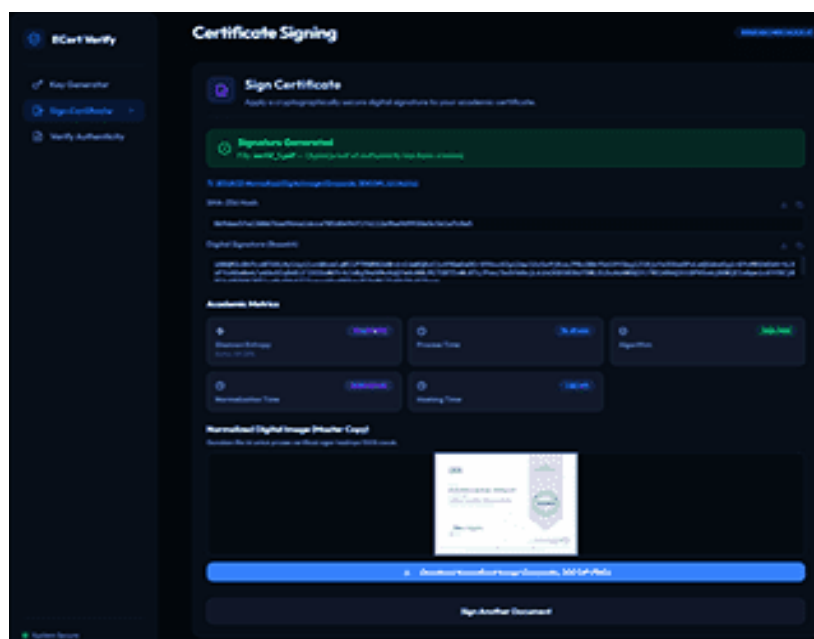
Dari Gambar 5, menu Sign Certificate menampilkan hasil penandatanganan digital yang telah berhasil dilakukan pada file *sertif_1.pdf*. Sistem secara otomatis melakukan normalisasi citra ke format Normalized Digital Image (Grayscale, 300 DPI) sebelum proses hashing dilakukan, lalu menghasilkan nilai hash SHA-256 sepanjang 64 karakter heksadesimal (256-bit). Pada bagian Academic Metrics, dihasilkan nilai Shannon Entropy sebesar 7,1467 bits dengan rasio keacakan 89,33%, total Process Time selama 76,25 ms, dan status penggunaan algoritma RSA-PSS. Data ini membuktikan bahwa sistem menghasilkan digital signature

yang kuat, acak, dan efisien sesuai standar kriptografi modern. Nilai Process Time sebesar 76,25 ms yang dihasilkan pada proses signing ini jauh lebih singkat dibandingkan proses Key Generation, mengkonfirmasi bahwa beban komputasi terbesar terletak pada tahap pembangkitan kunci yang hanya dilakukan sekali, sementara proses penandatanganan dokumen dapat dilakukan secara berulang dengan efisien.

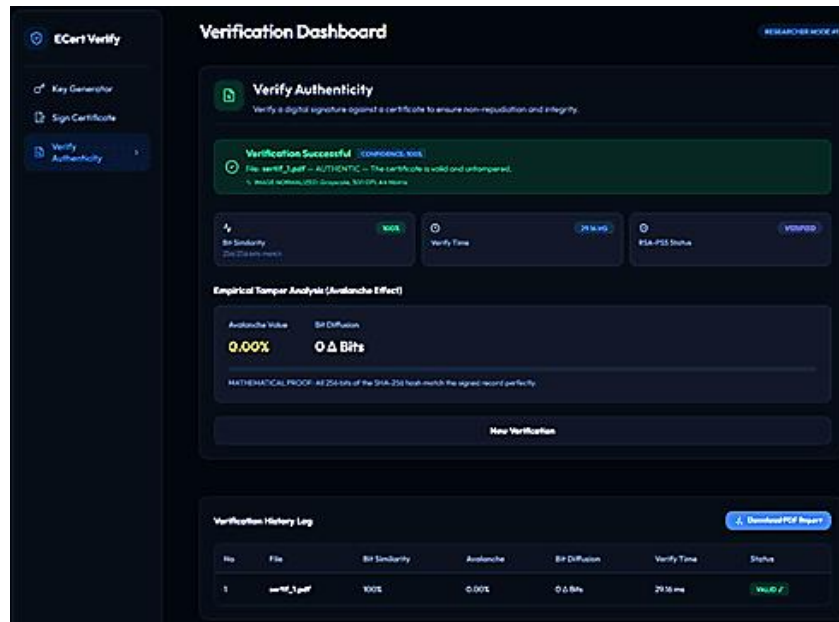
Selanjutnya, pengujian dilakukan dengan mengunggah kembali sertifikat yang sama ke menu Verify Authenticity untuk membuktikan bahwa sistem dapat mengenali keaslian dokumen yang telah ditandatangani. Hasil verifikasi terhadap file sertifikasi asli *sertif_1.pdf* ditunjukkan pada Gambar 6.

Berdasarkan Gambar 6, hasil verifikasi terhadap file sertifikat asli *sertif_1.pdf* menunjukkan status Verification Successful, AUTHENTIC dengan tingkat kepercayaan (*confidence*) sebesar 100%. Nilai Bit Similarity sebesar 100% (256/256 bits match) membuktikan bahwa seluruh 256 bit hash SHA-256 dari sertifikat yang diunggah identik dengan hash yang tersimpan dalam Digital Signature. Waktu verifikasi yang dibutuhkan hanya 13,76 ms, menunjukkan performa sistem yang sangat efisien. Pada bagian Empirical Tamper Analysis, nilai Avalanche Value sebesar 0,00% (0 Δ Bits) mengkonfirmasi secara matematis bahwa tidak ada satupun bit yang berubah pada file *sertif_1.pdf* sejak proses signing dilakukan.

Selanjutnya dilakukan pengujian terhadap kategori tampered untuk membuktikan kemampuan sistem dalam mendeteksi berbagai jenis manipulasi pada citra sertifikat. Tiga jenis manipulasi diujikan, yaitu: (1) screenshot layar sertifikat (*sertif_1_tampered_ss.png*), (2) kompresi ulang file PDF (*sertif_1_tampered_compress.pdf*), dan (3) modifikasi konten berupa perubahan teks pada citra sertifikat (*sertif_1_tampered_edit.png*). Contoh hasil verifikasi kategori tampered ditunjukkan pada Gambar 7. Berdasarkan Gambar 7, file hasil screenshot *sertif_1_tampered_ss.png* langsung terdeteksi sebagai INVALID dengan Confidence 0% dan Avalanche Value 58,59% (150 Δ Bits), membuktikan bahwa perubahan struktur byte akibat proses screenshot terdeteksi sepenuhnya oleh sistem. Hasil pengujian lengkap terhadap seluruh dataset tampered dirangkum pada Tabel II. Berdasarkan hasil pengujian pada Tabel II, sistem ECert Verify berhasil mengklasifikasikan seluruh 20 sampel file pengujian dengan tingkat akurasi 100%. Dari total 20 file, sebanyak 5 file sertifikat asli (*sertif_1.pdf* hingga *sertif_5.pdf*) dinyatakan VALID dengan nilai *Bit Similarity* 100% dan nilai *Avalanche Effect* 0.00%, sedangkan 15 file yang telah mengalami manipulasi dalam berbagai bentuk (*screenshot*, *kompresi*, dan *modifikasi langsung*) seluruhnya terdeteksi sebagai INVALID dengan *Bit Similarity* 0%.



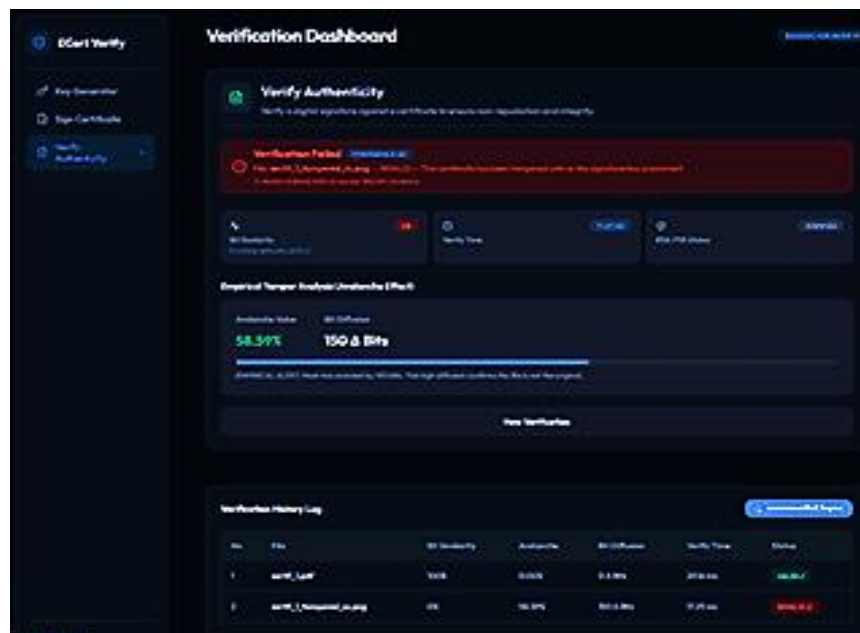
Gambar 5. Tampilan menu Sign Certificate pada Sistem ECert Verify



Gambar 6. Hasil Verifikasi VALID pada Sistem ECert Verify

Nilai *Avalanche Effect* pada seluruh file yang dimanipulasi menunjukkan rata-rata sebesar 50,88%, sangat mendekati nilai ideal 50% yang menjadi tolok ukur ketahanan fungsi hash SHA-256. Nilai tertinggi tercatat pada *sertif_1_tampered_ss.png* sebesar 58,59% (150 Δ Bits), sedangkan nilai terendah terdapat pada

sertif_4_tampered_modify.pdf sebesar 45,31% (116 Δ Bits). Distribusi nilai ini membuktikan bahwa perubahan sekecil apapun pada struktur byte citra sertifikat, termasuk perubahan akibat proses *screenshot* sekalipun, mampu menyebar secara merata ke seluruh bit nilai hash dan terdeteksi sepenuhnya oleh sistem.



Gambar 7. Contoh Hasil Verifikasi INVALID pada Sistem ECert Verify

TABEL II
HASIL PENGUJIAN VERIFIKASI SELURUH FILE

No	Nama File	Bit Similarity	Avalanche	Bit Diffusion	Time	Status
1	sertif_1.pdf	100%	0.00%	0 Δ Bits	29.16 ms	VALID
2	sertif_1_tampered_ss.png	0%	58.59%	150 Δ Bits	17.25 ms	INVALID
3	sertif_1_tampered_compressed.pdf	0%	47.27%	121 Δ Bits	3.13 ms	INVALID
4	sertif_1_tampered_modify.pdf	0%	57.81%	148 Δ Bits	2.14 ms	INVALID
5	sertif_2.pdf	100%	0.00%	0 Δ Bits	3.02 ms	VALID
6	sertif_2_tampered_ss.png	0%	49.61%	127 Δ Bits	3.70 ms	INVALID
7	sertif_2_tampered_compressed.pdf	0%	50.78%	130 Δ Bits	2.98 ms	INVALID
8	sertif_2_tampered_modify.pdf	0%	51.17%	131 Δ Bits	3.00 ms	INVALID
9	sertif_3.pdf	100%	0.00%	0 Δ Bits	2.09 ms	VALID
10	sertif_3_tampered_ss.png	0%	48.83%	125 Δ Bits	2.60 ms	INVALID
11	sertif_3_tampered_compressed.pdf	0%	48.05%	123 Δ Bits	2.25 ms	INVALID
12	sertif_3_tampered_modify.pdf	0%	52.73%	135 Δ Bits	2.32 ms	INVALID
13	sertif_4.pdf	100%	0.00%	0 Δ Bits	2.25 ms	VALID
14	sertif_4_tampered_ss.png	0%	51.56%	132 Δ Bits	3.18 ms	INVALID
15	sertif_4_tampered_compressed.pdf	0%	51.95%	133 Δ Bits	2.25 ms	INVALID
16	sertif_4_tampered_modify.pdf	0%	45.31%	116 Δ Bits	2.26 ms	INVALID
17	sertif_5.pdf	100%	0.00%	0 Δ Bits	2.17 ms	VALID
18	sertif_5_tampered_ss.png	0%	46.09%	118 Δ Bits	2.55 ms	INVALID
19	sertif_5_tampered_compressed.pdf	0%	54.69%	140 Δ Bits	2.20 ms	INVALID
20	sertif_5_tampered_modify.pdf	0%	48.83%	125 Δ Bits	2.19 ms	INVALID

Dari sisi performa, waktu eksekusi proses verifikasi seluruh file berada pada rentang 2,09 ms hingga 29,16 ms, dengan rata-rata waktu sebesar 4,57 ms. Waktu eksekusi tercepat dicapai pada *sertif_3.pdf* yaitu sebesar 2,09 ms, sedangkan waktu terlama tercatat pada *sertif_1.pdf* yang membutuhkan waktu 29,16 ms. Hal ini dipengaruhi oleh efek cold start, di mana sistem melakukan inisialisasi alokasi memori dan pemuatan pustaka kriptografi ke dalam lingkungan kerja pada eksekusi file pertama kali. Meskipun demikian performa waktu eksekusi secara umum berada di bawah 5 ms menunjukkan bahwa sistem ECert Verify memiliki kinerja yang sangat efisien dan layak diterapkan pada lingkungan pengujian single-user yang terkontrol.

Secara keseluruhan, hasil pengujian membuktikan bahwa kombinasi algoritma RSA-2048 dengan skema *padding* PSS dan fungsi hash SHA-256, yang diperkuat dengan proses normalisasi citra ke format *grayscale* 300 DPI, mampu mendeteksi seluruh bentuk manipulasi citra sertifikat secara akurat. Sistem ECert Verify tidak hanya mengandalkan perbandingan bit secara langsung, tetapi juga memanfaatkan sifat deterministik dari nilai *digital signature* yang dihasilkan, sehingga keaslian dan integritas dokumen dapat dipastikan secara kriptografis.

Lebih jauh, mekanisme verifikasi sistem ECert Verify beroperasi melalui dua lapisan kriptografis dengan tujuan yang berbeda secara fundamental. Lapisan pertama adalah Deteksi Integritas berbasis SHA-256, yang berfungsi mendeteksi perubahan pada level bit citra. Sifat Avalanche Effect SHA-256 menjamin bahwa manipulasi visual sekecil apapun akan menghasilkan nilai hash yang sepenuhnya berbeda dari hash awal saat sertifikat didaftarkan. Lapisan kedua adalah Autentikasi Sumber berbasis RSA-PSS, yang berfungsi mencegah pemalsuan signature. Bahkan jika

penyerang berhasil membuat citra palsu dan menghasilkan hash SHA-256 baru, penyerang tidak akan mampu membuat Digital Signature yang valid tanpa memiliki Private Key institusi penerbit. Kedua lapisan ini bekerja secara berurutan dalam modul *verify_signature*, di mana Public Key hanya akan mengembalikan status valid jika persamaan matematis RSA-PSS antara signature asli dan hash citra terpenuhi secara bersamaan.

Selain pengujian verifikasi, dilakukan pula pengujian Shannon Entropy terhadap nilai Digital Signature yang dihasilkan dari setiap sertifikat asli dalam dataset. Pengujian ini bertujuan untuk membuktikan secara empiris bahwa signature yang dihasilkan sistem ECert Verify memiliki tingkat keacakan yang tinggi sehingga tidak mengandung pola yang dapat dieksploitasi oleh penyerang. Hasil pengujian Shannon Entropy ditunjukkan pada Tabel III.

Berdasarkan Tabel III, seluruh file sertifikat asli menghasilkan nilai Shannon Entropy dengan rata-rata sebesar 7,1786 bits (89,73%), mendekati nilai maksimum teoritis 8,0 bits. Nilai tertinggi tercatat pada *sertif_3.pdf* sebesar 7,2385 bits (90,48%), sedangkan nilai terendah terdapat pada *sertif_1.pdf* sebesar 7,1467 bits (89,33%). Meskipun demikian, seluruh nilai berada dalam kategori *Sangat Baik* karena semuanya melampaui ambang batas 89%. Tingginya nilai entropy ini membuktikan bahwa *Digital Signature* yang dihasilkan sistem ECert Verify memiliki distribusi bit yang sangat acak. Penggunaan skema *padding* PSS pada RSA-2048 memberikan kontribusi signifikan karena PSS menambahkan unsur keacakan (*salt*) dalam setiap proses *signing*, sehingga *signature* untuk dokumen yang sama akan selalu berbeda setiap sesi namun verifikasi tetap berhasil menggunakan *Public Key* yang sesuai. Rekapitulasi hasil pengujian akurasi sistem dilakukan untuk merangkum kemampuan sistem ECert

Verify dalam mengklasifikasikan seluruh 20 data pengujian secara tepat. Hasil rekapitulasi akurasi verifikasi ditunjukkan pada Tabel IV.

Berdasarkan Tabel IV, sistem ECert Verify mencapai akurasi verifikasi sebesar 100% pada seluruh 20 data pengujian, tanpa ditemukan adanya kasus False Positive maupun False Negative. Hasil pengujian empiris ini konsisten dengan prinsip kerja SHA-256 yang bersifat *deterministic* dan *collision resistant*. Tidak adanya kesalahan klasifikasi pada seluruh sampel membuktikan bahwa sistem ECert Verify layak diterapkan sebagai solusi verifikasi keaslian sertifikat digital secara nyata.

TABEL III

HASIL PENGUJIAN SHANNON ENTROPY DIGITAL SIGNATURE

No	File Sertifikat	Shannon Entropy (bits)	Rasio Entropy (%)	Keterangan
1	sertif_1.pdf	7,1467	89,33%	Sangat Baik
2	sertif_2.pdf	7,1697	89,62%	Sangat Baik
3	sertif_3.pdf	7,2385	90,48%	Sangat Baik
4	sertif_4.pdf	7,1803	89,75%	Sangat Baik
5	sertif_5.pdf	7,1576	89,47%	Sangat Baik
	Rata-rata	7,1786	89,73%	Sangat Baik

TABEL IV

REKAPITULASI HASIL PENGUJIAN AKURASI VERIFIKASI

Kategori Pengujian	Total	Benar	Salah	Akurasi
Original — True Positive (TP)	5	5	0	100%
Tampered Screenshot — True Negative (TN)	5	5	0	100%
Tampered Kompresi — True Negative (TN)	5	5	0	100%
Tampered Modifikasi — True Negative (TN)	5	5	0	100%
Total Keseluruhan	20	20	0	100%

Selain pengujian akurasi, desain keamanan sistem ECert Verify secara inheren mengantisipasi beberapa skenario serangan kriptografis. Skenario modifikasi citra setelah signing telah dibuktikan melalui seluruh pengujian kategori tampered. Skenario forged signature dan perubahan public key ditangani secara matematis oleh RSA-2048, dibuktikan melalui pengujian unit test_wrong_public_key_fails_verification. Skenario signature substitution ditangani melalui pengujian test_tampered_signature_fails_verification. Untuk replay attack, sistem terlindungi secara inheren karena setiap signature terikat pada hash dokumen spesifik dan penambahan mekanisme nonce atau timestamp merupakan arah pengembangan yang direkomendasikan.

Terlepas dari aspek keamanan, sistem ECert Verify juga diuji dari sisi efisiensi performa waktu eksekusi. Pengujian dilakukan untuk menganalisis waktu eksekusi pada setiap tahapan proses kriptografi ECert Verify. Seluruh data waktu diperoleh langsung dari antarmuka sistem berdasarkan pengujian terhadap 5 sertifikat asli. Hasil pengujian waktu eksekusi ditunjukkan pada Tabel V.

Berdasarkan Tabel V, proses yang membutuhkan waktu paling lama adalah Normalisasi Citra dengan rata-rata 2.880,76 ms karena melibatkan konversi menyeluruh dari format PDF ke citra grayscale 300 DPI beresolusi tinggi (3508×2480 piksel). Proses Hashing SHA-256 berjalan sangat cepat dengan rata-rata hanya 2,03 ms, sedangkan

proses Signing RSA-2048 PSS membutuhkan rata-rata 79,08 ms per file. Proses Verification adalah yang paling cepat dengan rata-rata hanya 2,46 ms karena hanya memerlukan *re-hashing* dan pencocokan *signature* tanpa proses normalisasi berat. Keseluruhan waktu verifikasi yang berada di bawah 4 ms membuktikan bahwa sistem ECert Verify memiliki kinerja yang sangat efisien dan layak diterapkan pada lingkungan produksi berbasis web secara real-time. Klaim kelayakan real-time ini didasarkan pada pengujian single-user dalam lingkungan terkontrol, sehingga evaluasi lebih lanjut terhadap aspek concurrent users dan skalabilitas sistem diperlukan untuk memvalidasi kelayakan pada lingkungan produksi skala penuh. Selain itu, seluruh data hasil pengujian waktu eksekusi yang disajikan pada Tabel V ini merupakan nilai representatif yang diambil dari salah satu sesi pengujian sampel acuan untuk menunjukkan performa proses sistem secara komprehensif dari ujung ke ujung. Metrik rentang waktu dan rata-rata eksekusi ini akan selalu bersifat dinamis pada setiap pengujian sertifikat baru. Perubahan nilai waktu eksekusi riil secara pasti akan terjadi di lapangan karena dipengaruhi oleh variasi ukuran file, resolusi, serta ukuran byte dari masing-masing sertifikat yang diunggah, di samping faktor lokasi sumber daya komputasi dan beban kerja prosesor komputer sesaat ketika proses berjalan. Meskipun terjadi variasi nilai di setiap pengujian baru, performa sistem secara keseluruhan terbukti konsisten tetap berada pada skala milidetik (ms) yang sangat efisien.

TABEL V
HASIL PENGUJIAN WAKTU EKSEKUSI SISTEM ECERT VERIFY

No	Proses	Rentang Waktu (ms)	Rata-rata (ms)
1	Key Generation RSA-2048	103,30	103,30
2	Normalisasi Citra PDF ke Grayscale 300 DPI	2.487,50 – 3.274,71	2.880,76
3	Hashing SHA-256	1,79 – 2,63	2,03
4	Signing RSA-2048 PSS	72,28 – 93,76	79,08
5	Verification (Re-hash + Signature Matching)	2,08 – 3,77	2,46
	Total Waktu Signing (Proses 2+3+4)	2.561,57 – 3.371,10	2.961,87

D. Pengujian Limited User Acceptance Survey

Evaluasi utama penelitian ini berfokus pada pengujian kinerja algoritma digital signature RSA-PSS dan fungsi hash SHA-256. Pengujian User Acceptance Survey dilakukan secara terbatas sebagai evaluasi pendukung terhadap aspek operasional antarmuka yang digunakan oleh operator penerbit pada sistem ECert Verify. Survei ini melibatkan 10 responden yang berasal dari berbagai latar belakang lembaga pendidikan dan jurusan yang berbeda guna mendapatkan penilaian yang objektif. Penilaian dilakukan dengan menggunakan kuesioner yang mengevaluasi 8 indikator utama yang dinilai berdasarkan skala Likert (skor 1 sampai

5). Persentase kelayakan dari masing-masing indikator dihitung menggunakan rumus persamaan (9). Hasil pengumpulan data kuesioner dan perhitungan persentase kelayakan untuk ke-8 indikator disajikan pada Tabel VI. Dimana P = Persentase kelayakan akhir (%), $\sum x$ = Total skor aktual yang diberikan oleh seluruh responden, $\sum x_{max}$ = Skor maksimal ideal (Jumlah Responden $\times$ Skor Tertinggi Skala Likert = $10 \times 5 = 50$).

$$P = \frac{\sum x}{\sum x_{max}} \times 100\% \quad (9)$$

TABEL VI
HASIL PERHITUNGAN SKOR KUESIONER PENGGUNA

No	Indikator Penilaian	Skor Aktual ($\sum x$)	Skor Maksimal ($\sum x_{max}$)	Persentase Kelayakan (P)	Kategori
1	Antarmuka sistem mudah dipahami	46	50	92,00%	Sangat Layak
2	Proses pembuatan tanda tangan digital berjalan dengan baik	46	50	92,00%	Sangat Layak
3	Proses verifikasi sertifikat mudah dilakukan	46	50	92,00%	Sangat Layak
4	Informasi status valid/tidak valid mudah dipahami	44	50	88,00%	Sangat Layak
5	Sistem membantu proses validasi sertifikat digital	47	50	94,00%	Sangat Layak
6	Waktu respon sistem sudah memadai	48	50	96,00%	Sangat Layak
7	Menu-menu yang tersedia mudah digunakan	43	50	86,00%	Sangat Layak
8	Secara keseluruhan sistem dapat digunakan untuk mendukung proses penerbitan sertifikat	45	50	90,00%	Sangat Layak
	Total keseluruhan	365	400	-	-
	Rata-rata			91,25%	Sangat Layak

Berdasarkan Tabel VI, ke-8 indikator tersebut menampilkan pertanyaan-pertanyaan kuesioner yang secara spesifik diajukan kepada responden, yaitu: “Antarmuka sistem mudah dipahami.” (P1), “Proses pembuatan tanda tangan digital berjalan dengan baik.” (P2), “Proses verifikasi sertifikat mudah dilakukan.” (P3), “Informasi status valid/tidak valid mudah dipahami.” (P4), “Sistem membantu proses validasi sertifikat digital.” (P5), “Waktu respon sistem sudah memadai.” (P6), “Menu-menu yang tersedia mudah digunakan.” (P7), serta “Secara keseluruhan sistem dapat digunakan untuk mendukung proses penerbitan sertifikat.” (P8).

Hasil dari analisis data menunjukkan bahwa indikator waktu respon sistem (P6) mendapatkan skor tertinggi dari para responden dengan persentase mencapai 96,00%. Ini membuktikan sistem ECert Verify berjalan dengan lancar dan cepat. Di sisi yang lain, indikator kemudahan menu-menu yang tersedia (P7) mencatatkan nilai terendah 86,00%. Meskipun begitu, semua elemen pengujian tetap berada pada tingkat penilaian yang sangat baik.

Secara keseluruhan, tes Limited User Acceptance Survey yang melibatkan 10 responden ini menghasilkan nilai rata-rata persentase kelayakan akhir sebesar 91,25%. Berdasarkan kriteria penilaian skor dari skala Likert, nilai keseluruhan tersebut masuk ke dalam kategori “Sangat Layak”. Melalui

hasil ini, dapat diambil kesimpulan bahwa platform ECert Verify berbasis kriptografi RSA dan SHA-256 yang dikembangkan telah memenuhi ekspektasi kegunaan, fungsi sistem, dan diterima dengan sangat baik oleh responden pengujian untuk diaplikasikan dalam situasi operasional nyata.

E. Perbandingan dengan Penelitian Terdahulu

Untuk mengevaluasi performa dan keandalan sistem ECert Verify, dilakukan analisis komparatif antara hasil pengujian sistem yang dikembangkan dengan beberapa penelitian terdahulu yang relevan. Parameter perbandingan mencakup pendekatan arsitektur, objek pemrosesan, metode standarisasi citra, keandalan kriptografi, serta efisiensi waktu verifikasi seperti yang ditampilkan di Tabel VII. Berdasarkan analisis komparatif pada Tabel VII, penelitian terdahulu seperti Kontzinos dkk. [14], Satybaldy dkk. [15], Baniata dkk. [16] berfokus pada arsitektur terdistribusi untuk data teks/metadate tanpa menerapkan prapemrosesan citra dan menguji ketahanan terhadap manipulasi visual (tampering). Sistem ECert Verify berhasil mengatasi keterbatasan tersebut melalui normalisasi citra grayscale 300 DPI, yang terbukti mencapai akurasi 100% dalam mendeteksi screenshot,

kompresi ulang, dan modifikasi konten dengan sensitivitas Avalanche Effect sebesar 50,88%. Dari aspek efisiensi, sistem ECert Verify mencatatkan rata-rata waktu verifikasi yang sangat cepat yaitu 2,46 ms per file, jauh lebih unggul dibandingkan penelitian [16] (3 ms – 140 ms). Hal ini membuktikan bahwa pendekatan web terpusat berbasis RSA-2048 (RSASSA-PSS) dan SHA-256 yang dikembangkan sangat efisien dan andal untuk verifikasi keaslian dokumen secara real-time.

Meskipun demikian, perlu diakui bahwa penelitian ini memiliki keterbatasan dalam hal ukuran dataset yang diuji (5 sertifikat asli dan 15 variasi manipulasi). Pembatasan ini dipicu oleh aspek privasi data (data privacy), karena seluruh sampel yang digunakan merupakan dokumen kredensial pribadi milik penulis yang diperoleh secara sah dari platform Coursera demi mematuhi etika perlindungan informasi personal. Namun, skala pengujian terbatas ini telah memadai sebagai validasi awal (proof-of-concept) mengingat karakteristik matematis SHA-256 yang sensitif terhadap avalanche effect secara teoritis menjamin konsistensi deteksi pada tingkat biner. Evaluasi dengan volume data yang lebih masif direkomendasikan untuk penelitian selanjutnya guna menguji stabilitas komputasi pada skala industri.

TABEL VII

PERBANDINGAN HASIL DAN KARAKTERISTIK SISTEM ECERT VERIFY DENGAN PENELITIAN TERDAHULU

Parameter	Kontzinos dkk. [14]	Satybaldy dkk. [15]	Baniata dkk. [16]	Penelitian ini (ECert Verify)
Pendekatan Arsitektur	Blockchain (QualiChain)	Self-Sovereign Identity	Fog-Blockchain (PriFoB)	Aplikasi Web Terpusat / Klien-Server (Lightweight)
Objek Data Utama	Metadata Dokumen	Kredensial JSON-LD	Data Kredensial DID	Citra Hasil Konversi PDF (Grayscale 300 DPI)
Standarisasi Citra	Tidak Ada	Tidak Ada	Tidak Ada	Normalisasi Grayscale 300 DPI (3508 × 2480 px)
Keandalan Kriptografi	Smart Contract Hash	Digital Signature	Asymmetric Key (RSA)	RSA-2048 (RSASSA-PSS) + SHA 256
Rata-rata Waktu Verifikasi	Tidak Dilaporkan	Tidak Dilaporkan	0,003 s – 0,14 s (3 ms – 140 ms)	2,46 ms
Deteksi Manipulasi Citra (Tampering)	Tidak Diuji	Tidak Diuji	Tidak Diuji	Akurasi 100% (Sensitif Avalanche Effect 50,88%)

IV. KESIMPULAN

Penelitian ini berhasil mengimplementasikan mekanisme digital signature berbasis algoritma RSA-2048 dengan skema padding PSS (*Probabilistic Signature Scheme*) dan fungsi hash SHA-256 pada sistem ECert Verify untuk memverifikasi keaslian citra sertifikat digital secara otomatis. Berdasarkan hasil pengujian yang telah dilakukan, dapat ditarik beberapa kesimpulan sebagai berikut.

Pertama Sistem ECert Verify mampu mendeteksi seluruh bentuk manipulasi citra sertifikat dengan tingkat akurasi 100% pada 20 data pengujian yang terdiri dari 5 sertifikat asli dan 15 variasi tampered (screenshot, kompresi ulang, dan modifikasi konten), tanpa terdapat kasus False Positive maupun False Negative pada dataset pengujian yang

digunakan. Kedua Nilai Avalanche Effect rata-rata sebesar 50,88% pada seluruh file yang dimanipulasi membuktikan bahwa fungsi hash SHA-256 memiliki sensitivitas tinggi terhadap perubahan sekecil apa pun pada struktur byte citra sertifikat, mendekati nilai ideal 50% yang menjadi standar ketahanan kriptografi. Ketiga pengujian Shannon Entropy menghasilkan rata-rata sebesar 7,1786 bits (89,73%), membuktikan bahwa digital signature yang dihasilkan sistem ECert Verify memiliki distribusi bit yang sangat acak dan tidak mengandung pola yang dapat dieksploitasi oleh penyerang. Proses normalisasi citra ke format grayscale 300 DPI sebelum proses hashing terbukti efektif dalam memastikan konsistensi nilai hash SHA-256 untuk setiap file yang identik, terlepas dari platform atau perangkat yang digunakan. Keempat, berdasarkan hasil pengujian pendukung melalui User Acceptance Survey terbatas yang melibatkan 10

responden operator, sistem ECert Verify memperoleh rata-rata persentase kelayakan akhir sebesar 91,25% yang termasuk ke dalam kategori “Sangat Layak”. Hasil ini menunjukkan bahwa sistem telah memenuhi ekspektasi kegunaan, fungsionalitas, serta dapat diterima dengan sangat baik oleh responden pengujian untuk mendukung aspek operasional penerbitan sertifikat.

Sistem ECert Verify menunjukkan performa yang sangat efisien dengan rata-rata waktu verifikasi hanya 2,46 ms per file pada lingkungan pengujian single-user yang terkontrol. Evaluasi lebih lanjut terhadap aspek concurrent users dan skalabilitas diperlukan sebelum sistem diterapkan pada lingkungan produksi skala penuh. Untuk mendukung pengembangan, terdapat beberapa saran yang dapat dipertimbangkan untuk penelitian selanjutnya. Mengintegrasikan sistem ECert Verify dengan teknologi blockchain sebagai penyimpanan digital signature yang terdesentralisasi, sehingga proses verifikasi dapat dilakukan secara offline tanpa bergantung pada koneksi ke server pusat. Mengembangkan fitur batch verification yang memungkinkan verifikasi banyak sertifikat sekaligus dalam satu sesi, sehingga meningkatkan efisiensi bagi institusi yang memerlukan verifikasi dokumen dalam jumlah besar. Menambahkan mekanisme pencabutan tanda tangan (*signature revocation*) untuk menangani skenario di mana Private Key penerbit telah dikompromikan atau sertifikat perlu dibatalkan sebelum masa berlakunya habis. Memperluas cakupan evaluasi keamanan dengan mengintegrasikan mekanisme nonce atau timestamp dinamis guna memperkuat pertahanan sistem terhadap potensi serangan replay attack secara real-time.

DAFTAR PUSTAKA

- [1] P. A. P. Mabotha and B. S. Ngcamu, “Digital Transformation in the Higher Education Sector: A Systematic Literature Review,” *Adm. Sci.*, vol. 16, no. 1, p. 1, Dec. 2025, doi: 10.3390/admsci16010001.
- [2] P. Boulet, P. de Coëtlogon, É. Thébault, P. van de Velde, and C. Murie, “Digital transformation of certificates issued by universities for European competitiveness(Technical Report),” Mar. 2025. [Online]. Available: https://commission.europa.eu/resources-partners/etranslation_fr
- [3] M. Alenezi and M. Akour, “Digital Transformation Blueprint in Higher Education: A Case Study of PSU,” *Sustainability (Switzerland)*, vol. 15, no. 10, May 2023, doi: 10.3390/su15108204.
- [4] A. Nigmatov, A. Pradeep, and N. Musulmonova, “Blockchain Technology in Improving Transparency and Efficiency in Government Operations,” in *15th International Conference on Electronics, Computers and Artificial Intelligence, ECAI 2023 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., May 2024. doi: 10.1109/ECAI58194.2023.10194154.
- [5] A. Noor, B. Wassir, I. Anggraini, and E. Rahmaniah, “Implications of the Use of Electronic Certificates in Proving Land Rights According to the Civil Procedure Law,” *Electronic Journal of Education, Social Economics and Technology*, vol. 5, no. 2, pp. 276–281, Oct. 2024, doi: 10.33122/ejeset.v5i2.266.
- [6] I. E. Khairuddin, N. A. Safian, M. K. Zaini, and N. Ahmad Uzir, “Navigating Academic Credentials in the Digital Age: Insights, Challenges, and Implications for Graduates,” *Journal of Ecohumanism*, vol. 3, no. 4, pp. 642–651, Aug. 2024, doi: 10.62754/joe.v3i4.3492.
- [7] S. Boonkrong, “Design of an academic document forgery detection system,” *International Journal of Information Technology (Singapore)*, vol. 17, no. 9, pp. 5175–5187, Dec. 2025, doi: 10.1007/s41870-024-02006-6.
- [8] O. S. Saleh, O. Ghazali, and M. E. Rana, “Blockchain based framework for educational certificates verification,” 2020, *Innovare Academics Sciences Pvt. Ltd.* doi: 10.31838/jcr.07.03.13.
- [9] H. Reddy Penubadi *et al.*, “Sustainable electronic document security: a comprehensive framework integrating encryption, digital signature and watermarking algorithms,” *Heritage and Sustainable Development*, vol. 5, no. 2, pp. 391–404, 2023, doi: 10.37868/hsd.v4i1.359.
- [10] P. Kiiskilä, A. Kukkonen, and H. Pirkkalainen, “Are Micro-Credentials Valuable for Students? Perspective on Verifiable Digital Credentials,” *SN Comput. Sci.*, vol. 4, no. 4, Jul. 2023, doi: 10.1007/s42979-023-01797-y.
- [11] Jamil, “The Implementation of Electronic Certificates in Public Administration: Towards a Legal Framework that Supports Digital Inclusivity,” 2025, doi: 10.33830/osc.v3i1.7054/ISSN.
- [12] M. Al Hemaury, M. Abu Talib, A. Khalil, A. Zulfiqar, and T. Mohamed, “Blockchain-based framework and platform for validation, authentication & equivalency of academic certification and institution’s accreditation: UAE case study and system performance (2022),” *Educ. Inf. Technol. (Dordr.)*, vol. 29, no. 14, pp. 18203–18232, Oct. 2024, doi: 10.1007/s10639-024-12493-6.
- [13] M. Zanardelli, F. Guerrini, R. Leonardi, and N. Adami, “Image forgery detection: a survey of recent deep-learning approaches,” *Multimed. Tools Appl.*, vol. 82, pp. 17521–17566, Oct. 2022, doi: 10.1007/s11042-022-13797-w.
- [14] C. Kontzinos, E. Karakolis, P. Kokkinakos, S. Skolidakis, D. Askounis, and J. Psarras, “Application and Evaluation of a Blockchain-Centric Platform for Smart Badge Accreditation in Higher Education Institutions,” *Applied Sciences (Switzerland)*, vol. 14, no. 12, Jun. 2024, doi: 10.3390/app14125191.
- [15] A. Satybaldy, A. Subedi, and M. Nowostawski, “A Framework for Online Document Verification Using Self-Sovereign Identity Technology,” *Sensors*, vol. 22, no. 21, Nov. 2022, doi: 10.3390/s22218408.
- [16] H. Baniata and A. Kertesz, “PriFoB: A Privacy-aware Fog-enhanced Blockchain-based system for Global Accreditation and Credential Verification,” *Journal of Network and Computer Applications*, vol. 205, Sep. 2022, doi: 10.1016/j.jnca.2022.103440.
- [17] A. O. Mulani, V. V. Godase, S. R. Takale, and R. G. Ghodake, “Image Authentication Using Cryptography and Watermarking,” Sep. 2025.
- [18] H. Abdul and H. Khalid, “Instantaneous Documents Authentication and Verification based on Robust Digital Signature 4,” *International Journal of Computational Intelligence in Control*, vol. 14, no. 1, Jun. 2022.
- [19] A. Saputra and R. Purba, “Integration of ECDHE Curve25519, RSASSA-PSS, and AES-256 for Enhanced PrivateDH Key Exchange Protocol in End-to-End Communication,” *Journal of Novel Engineering Science and Technology*, vol. 4, no. 03, pp. 106–121, Dec. 2025, doi: 10.56741/jnest.v4i03.1275.
- [20] M. N. Arifin, M. Umar Mansyur, A. Rahman, N. P. Dewi, and F. P. E. Putra, “Enhanced OCR Recognition for Madurese Text Documents: A Genetic Algorithm Approach with Tesseract 5.5,” Jul. 2025.
- [21] M. Merkepci, H. Merkepci, and A. Ioanid, “Symbolic Plithogenic Numbers in RSA Cryptography: A Path to Post-Quantum Security,” *IEEE Access*, vol. 13, pp. 176110–176118, 2025, doi: 10.1109/ACCESS.2025.3620040.