PENERAPAN ALGORITMA KRIPTOGRAFI SHA-256 DAN TEKNOLOGI *BLOCKCHAIN* UNTUK KEAMANAN CITRA DIGITAL

LAPORAN TUGAS AKHIR

Laporan ini disusun guna memenuhi salah satu syarat untuk menyelesaikan program studi Teknik Informatika S-1 pada Fakultas Teknologi Industri Universitas Islam Sultan Agung

DISUSUN OLEH :

SILVIA PUTRI ANGGRAENI

NIM 32602100116

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS ISLAM SULTAN AGUNG

SEMARANG

2025

FINAL PROJECT

APPLICATION OF SHA-256 ALGORITHM CRYTOPRAPHIC AND BLOCKCHAIN TECHNOLOGY FOR DIGITAL IMAGE SECURITY

This Final Assignment Report was prepared as one of the requirements for obtaining a Bachelor's Degree (S1) in the Informatics Engineering Study Program, Sultan Agung Islamic University, Semarang.

Arranged By :

SILVIA PUTRI ANGGRAENI

NIM 32602100116

MAJORING OF INFORMATICS ENGINEERING

INDUSTRIAL TECHNOLOGY FACULTY

SULTAN AGUNG ISLAMIC UNIVERSITY

SEMARANG

2025

LEMBAR PENGESAHAN

TUGAS AKHIR

PENERAPAN ALGORITMA KRIPTOGRAFI SHA-256 DAN TEKNOLOGI *BLOCKCHAIN* UNTUK KEAMANAN CITRA DIGITAL

SILVIA PUTRI ANGGRAENI

32602100116

Telah dipertahankan di depan tim penguji ujian sarjana tugas akhir

Program Studi Teknik Informatika

Universitas Islam Sultan Agung

Pada tanggal : 24 Februari 2025

TIM PENGUJI UJIAN SARJANA:

Badie'ah, ST, M.Kom		
NIDN. 0619018701	.....	13-03-2025
(Ketua Penguji)		
Andi Riansyah, ST, M.Kom		
NIDN. 0609108802	.....	11-03-2025
(Anggota Penguji)		
Bagus SWP, S.Kom, M.Cs		
NIDN. 210616051	.....	11-03-2025
(Pembimbing)		

Semarang, ...

Mengetahui,

Kaprodi Teknik Informatika

Universitas Islam Sultan Agung

Moch. Taufik, ST., MIT

NIDN. 0622037502

SURAT PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertanda tangan dibawah ini :

Nama : Silvia Putri Anggraeni

NIM : 32602100116

Judul Tugas Akhir : Penerapan Algoritma Kriptografi SHA-256 dan Teknologi *Blockchain* Untuk Keamanan Citra Digital

Dengan bahwa ini saya menyatakan bahwa judul dan isi Tugas Akhir yang saya buat dalam rangka menyelesaikan Pendidikan Strata Satu (S1) Teknik Informatika tersebut adalah asli dan belum pernah diangkat, ditulis ataupun dipublikasikan oleh siapapun baik keseluruhan maupun sebagian, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka, dan apbila di kemudian hari ternyata terbukti bahwa judul Tugas Akhir tersebut pernah diangkat, ditulis ataupun dipublikasikan, maka saya bersedia dikenakan sanksi akademis. Demikian surat pernyataan ini saya buat dengan sadar dan penuh tanggung jawab.

Semarang, 13 Maret 2025

Yang Menyatakan,

Silvia Putri Anggareni

PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH

Saya yang bertanda tangan dibawah ini :

Nama : Silvia Putri Anggraeni

NIM : 32602100116

Program Studi : Teknik Informatika

Fakultas : Teknologi industri

Dengan ini menyatakan Karya Ilmiah berupa Tugas akhir dengan Judul : Penerapan Algoritma Kriptografi SHA-256 dan Teknologi *Blockchain* Untuk Keamanan Citra Digital.

Menyetujui menjadi hak milik Universitas Islam Sultan Agung serta memberikan Hak bebas Royalti Non-Eksklusif untuk disimpan, dialihmediakan, dikelola dan pangkalan data dan dipublikasikan diinternet dan media lain untuk kepentingan akademis selama tetap menyantumkan nama penulis sebagai pemilik hak cipta. Pernyataan ini saya buat dengan sungguh-sungguh. Apabila dikemudian hari terbukti ada pelanggaran Hak Cipta/Plagiarisme dalam karya ilmiah ini, maka segala bentuk tuntutan hukum yang timbul akan saya tanggung secara pribadi tanpa melibatkan Universitas Islam Sultan agung.

Semarang, 13 Maret 2025

Yang menyatakan,

Silvia Putri Anggraeni

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

ABSTRAK

Sistem keamanan digital berbasis *blockchain* dan AI dikembangkan untuk verifikasi sertifikat akademik secara otomatis, menggantikan proses manual yang rentan pemalsuan dan memakan waktu lama. Sistem ini memanfaatkan AI-OCR berbasis *Deep Learning* untuk mengekstrak teks dari sertifikat, lalu menggunakan algoritma SHA-256 untuk menghasilkan *hash* gambar berdasarkan struktur piksel serta *hash* teks berdasarkan isi dokumen, yang kemudian disimpan di *database* dan *blockchain* guna memastikan keasliannya. Dengan dataset lebih dari 200 sertifikat asli dalam format PNG dan JPG, sertifikat diproses melalui *grayscale* dan *resize* sebelum *hashing* dan penyimpanan. Pengujian menunjukkan bahwa *hash* gambar memiliki kesesuaian 100% dengan yang tersimpan di *blockchain*, sementara verifikasi teks OCR mencapai akurasi 100%, membuktikan bahwa sistem ini mampu memverifikasi sertifikat secara cepat, aman, dan akurat. Integrasi AI-OCR juga meningkatkan efisiensi dibandingkan metode manual, sehingga penelitian ini diharapkan menjadi solusi anti-pemalsuan yang dapat diterapkan di institusi akademik dan organisasi lain yang membutuhkan sistem verifikasi dokumen digital yang andal dan transparan.

Kata Kunci : *Blockchain*, AI-OCR, SHA-256, Keamanan Digital

ABSTRACT

A blockchain and AI-based digital security system was developed for automatic academic certificate verification, replacing the manual process that is prone to forgery and time-consuming. This system utilizes deep learning-based AI-OCR to extract text from certificates, then applies the SHA-256 algorithm to generate an image hash based on pixel structure and a text hash based on document content, which are then stored in a database and blockchain to ensure authenticity. With a dataset of over 200 original certificates in PNG and JPG formats, certificates are processed through grayscale conversion and resizing before hashing and storage. Testing results show that the image hash achieves 100% consistency with the blockchain-stored data, while OCR text verification reaches an accuracy of 98.6%, proving that this system can verify certificates quickly, securely, and accurately. The integration of AI-OCR also enhances efficiency compared to manual methods, making this research a promising anti-counterfeiting solution that can be applied in academic institutions and other organizations requiring a reliable and transparent digital document verification system.

Keywords: Blockchain, AI-OCR, SHA-256, Digital Security

BAB I
PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi pada saat ini sudah sangat banyak sekali kita temukan, terutama pada bidang kecerdasan buatan (AI). AI hadir menghadirkan tantangan baru dalam berbagai bidang teknologi, salah satunya dalam bidang keamanan citra digital. Dengan semakin berkembangnya aplikasi maupun web di bidang kecerdasan buatan (AI) dalam berbagai sektor, seperti pengenalan wajah, analisis citra medis, dan forensik digital, perlindungan terhadap manipulasi atau pemalsuan data citra menjadi krusial. Serangan yang menargetkan sistem AI melalui gambar yang dimodifikasi dapat menyebabkan kegagalan sistem atau hasil analisis yang salah. Oleh karena itu, diperlukan metode keamanan yang lebih kuat untuk melindungi keutuhan dan autentisitas data citra digital yang digunakan dalam sistem AI.

Teknologi *blockchain* hadir sebagai salah satu Solusi untuk meningkatkan keamanan citra digital dalam sistm AI. *Blockchain* terkenal dengan desentralisasi dan integritasnya, transparansi dan yang utama sifatnya tidak dapat diubah pada rantai blok yang sudah ada di *blockchain.* Dengan algoritma OCR *Deep Learning* (*Optical Character Recognition*) dan SHA-256 (*Secure Hash Algorithm 256*), *blockchain* dapat digunakan untuk memastikan keaslian citra digital. OCR (*Optical Character Recognition*) digunakan untuk meningkatkan akurasi dalam membaca teks dari sertifikat atau citra digital. OCR (Optical Character Recognition) yang digunakan adalah model *Deep Learning* menggunakan EasyOCR, dimana sistem akan lebih fleksibel dalam mengenali karakter di citra digital. Dan SHA-256 digunakan sebagai sidik digital unik, sehingga setiap perubahan data atau apabila terjadi manipulasi citra digital akan terdeteksi.

Penelitian ini memiliki tujuan untuk mengembangkan sistem keamanan citra digital yang didukung oleh OCR *Deep Learning* untuk

memverifikasi dan memproses citra digital, algoritma SHA-256 untuk menghasilkan kode unik dari masing-masing citra digital, dan keamanannya disimpan di *blockchain.*

1.2 Perumusan Masalah

Berdasarkan pernyataan latar belakang permasalahan yang telah diuraikan diatas, dapat diidentifikasi permasalahan dalam penelitian ini, yaitu :

1. Bagaimana teknologi *blockchain* dapat digunakan untuk menjamin keamanan citra digital?
2. Bagaimana Algoritma SHA-256 dapat diimplementasikan dalam *blockchain* untuk menjamin integritas dan keaslian citra digital?
3. Bagaimana integrasi antara *blockchain* dan OCR AI dapat memperkuat keamanan serta efisiensi pengelolaan data citra digital?

1.3 Pembatasan Masalah

Sesuai dengan rumusan masalah diatas, berikut ini merupakan batasan masalah yaitu :

1. Penelitian ini akan fokus pada jenis *blockchain* tertentu, yaitu *private blokchain*.
2. Jenis citra digital yang digunakan sebagai dataset maupun pengujian sistem hanya berupa gambar, tidak mencakup semua jenis data visual.
3. Serangan keamanan pada penelitian ini hanya fokus terhadap manipulasi atau pemalsuan data citra digital.

1.4 Tujuan

Adapun tujuan dari penelitian ini yaitu sebagai berikut:

1. Membangun dan mengembangkan sistem yang dapat melindungi citra digital dari manipulasi maupun pemalsuan data dengan menggunakan teknologi *blockhain*.
2. Menerapkan algoritma SHA-256 untuk keamanan citra digital

3. Mengurangi resiko pemalsuan citra digital dengan sistem berbasis *blockchain.*

1.5 Manfaat

Berdasarkan permasalahan dan tujuan yang telah diuraikan, penelitian ini diharapkan dapat memberikan manfaat untuk meningkatkan keamanan dan keabsahan sertifikat digital dengan teknologi SHA-256, AI-OCR, dan *Blockchain*, sehingga mencegah pemalsuan dan memastikan sertifikat tetap autentik.

1.6 Sistematika Penulisan

Adapun sistematika penulisan yang akan digunakan dalam pembuatan laporan tugas akhir ini adalah sebagai berikut :

BAB I : PENDAHULUAN

Pada bab I berisi penjelasan mengenai latar belakang pemilihan judul penelitian, perumusan masalah, pembatasan masalah, tujuan penelitian, manfaat penelitian, serta sistematika penulisan.

BAB II : TINJAUAN PUSTAKA DAN DASAR TEORI

Pada bab II berisi tentang penjelasan pada penelitian – penelitian sebelumnya dan dasar teori yang berhubungan dengan OCR, *Blockchain* maupun SHA-256 sebagai referensi peneliti untuk menulis penelitian ini.

BAB III : METODE PENELITIAN

Pada bab ini dijelaskan proses serta tahapan – tahapan penelitian mulai dari pengumpulan data hingga proses pengolahan data.

BAB IV : HASIL DAN ANALISIS PENELITIAN

Pada bab ini dijelaskan proses serta tahapan – tahapan penelitian mulai dari pengumpulan data hingga proses pengolahan data.

BAB V : KESIMPULAN DAN SARAN

Bab lima berisi dari kesimpulan proses penelitian dari awal proses penelitian hingga akhir penelitian.

BAB II
TINJAUAN PUSTAKA DAN DASAR TEORI

2.1 Tinjauan Pustaka

Beberapa penelitian sebelumnya telah mengkaji serta menerapkan teknologi *blockchain* dengan berbagai metode dan teknologi.

Penerapan teknologi *blockchain* di Kementerian Agraria dan Tata Ruang Badan Pertanahan Nasional berpotensi mencegah serta mengatasi permasalahan sertifikat tanah ganda. Mengingat bahwa teknologi ini masih dalam tahap pengembangan, diperlukan evaluasi untuk menentukan aspek yang dapat diadopsi serta perbaikan yang perlu dilakukan agar selaras dengan regulasi yang berlaku di Indonesia(Joshua P Nugraha).

Sistem verifikasi dokumen ijazah dapat memanfaatkan teknologi *blockchain* untuk mengidentifikasi ijazah digital. Proses ini dilakukan dengan membandingkan citra menggunakan perhitungan PSNR, di mana jika nilai yang diperoleh melebihi 40, citra tersebut dianggap identik. Dengan demikian, teknologi ini dapat digunakan sebagai metode validasi keaslian ijazah secara digital(Alfina & Syafrinal, 2022a)

Penerapan teknologi *blockchain* dengan *Smart contract* dan *distributed ledger* pada *platform Edutech* telah terbukti mampu meningkatkan keamanan, transparansi, dan efisiensi dalam pengelolaan sertifikat pendidikan. Dengan adanya otomatisasi dan desentralisasi melalui kontrak pintar serta jaminan integritas data dari *distributed ledger*, sistem ini dapat mengurangi risiko pemalsuan dan meningkatkan kepercayaan terhadap sertifikat yang diterbitkan. Oleh karena itu, teknologi *blockchain* memiliki potensi besar dalam merevolusi manajemen sertifikat pendidikan, memberikan manfaat signifikan dalam memastikan keamanan dan integritas data pada *platform* Edutech(Oknora Firza & Ilmu Komputer, 2024)

Penelitian ini menggunakan pendekatan studi kasus untuk menganalisis potensi penerapan teknologi *blockchain* dalam meningkatkan transparansi dan keamanan rantai pasokan industri kelapa sawit. Pengumpulan data dilakukan melalui wawancara dengan para ahli industri, observasi langsung di lapangan,

serta analisis dokumen terkait. Selanjutnya, analisis kualitatif digunakan untuk mengidentifikasi temuan utama dalam penelitian ini(Iqbal Adriansyah., 2024).

Dalam proses audit, *blockchain* menyediakan fitur seperti pencatatan permanen, pencegahan transaksi ganda, kontrak pintar, *triple-entry accounting*, dan enkripsi transaksi, yang membuat berbagai bentuk kecurangan lebih sulit dilakukan. Salah satu contoh penerapannya adalah *platform* yang meningkatkan transparansi serta keamanan pencatatan transaksi, seperti yang dikembangkan oleh *Blockchain* Intelligence Group (BIG). *Platform* ini menawarkan solusi audit digital dengan jejak audit yang tidak dapat diubah, sehingga mendukung proses deteksi dan investigasi kecurangan(Syahronny & Dewayanto, 2024)

Teknologi *blockchain* dalam sektor keuangan Islam memungkinkan berbagai penerapan, seperti penggunaan kontrak pintar, pengelolaan zakat, serta pengembangan rantai pasokan halal yang lebih produktif, efisien, dan efektif. Selain itu, *blockchain* juga dapat dimanfaatkan untuk mengoptimalkan sukuk ritel. Meskipun berfungsi sebagai buku besar terdistribusi, teknologi ini dapat dikelola secara privat oleh bisnis dan organisasi dengan membatasi jumlah peserta dalam transaksi. Masterplan Ekonomi Syariah 2019-2024 mendukung penerapan *blockchain*, sementara Indonesia juga memperoleh manfaat demografis yang berharga untuk mengakselerasi perkembangan teknologi ini(Arwani & Priyadi, 2024).

Hasil analisis penelitian terhadap sistem e-sertifikat berbasis *blockchain* menunjukkan bahwa sistem ini mampu memberikan hasil yang akurat dan mendukung otomatisasi proses sertifikasi bagi mahasiswa, instansi, serta perguruan tinggi. Dari penelitian tersebut, dapat disimpulkan tiga hal utama, pertama, sistem e-sertifikat saat ini sudah diterapkan di perguruan tinggi, namun belum berjalan secara optimal. Kedua, masih terdapat celah yang memungkinkan manipulasi oleh pihak yang tidak bertanggung jawab dan ketiga, diperlukan peningkatan sistem untuk memastikan keamanan dan keandalan dalam verifikasi sertifikat.

Penerapan sistem e-sertifikat berbasis teknologi *blockchain* oleh suatu instansi dapat mempermudah proses secara real-time dengan tingkat akurasi

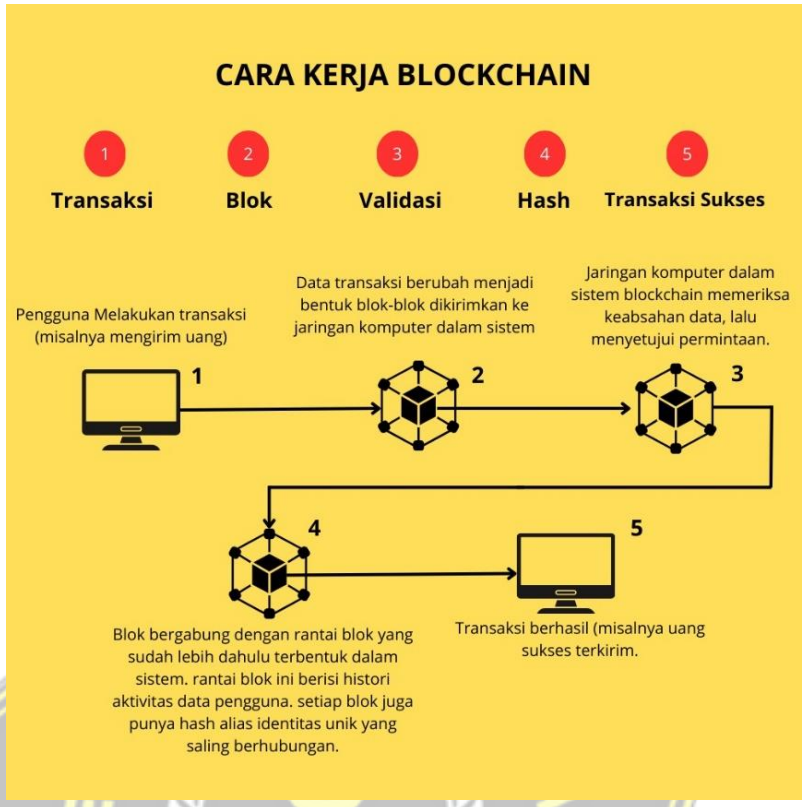
dan keamanan yang tinggi. Teknologi ini juga mampu mencegah terjadinya manipulasi data. Dengan adanya perangkat lunak e-sertifikat berbasis *blockchain*, proses pencocokan data dapat dilakukan secara otomatis, sehingga e-sertifikat menjadi lebih aman dan andal(Argani & Taraka)

2.2 Dasar Teori

2.2.1 *Blockchain*

Blockchain adalah sistem pencatatan informasi serta tidak dapat untuk mengubah, meretas, atau menipu. *Blockchain* pada dasarnya adalah buku besar transaksi digital yang diduplikasi dan didistribusikan ke seluruh jaringan sistem komputer di *blockchain*. Setiap blok dalam rantai berisi sejumlah transaksi, dan setiap kali transaksi baru terjadi di *blockchain*, catatan transaksi tersebut ditambahkan ke buku besar setiap pemilik atau pemegang lainnya . Basis data terdesentralisasi yang dikelola oleh banyak peserta dikenal sebagai *Distributed Ledger* Technology (DLT)(Alfina & Syafrinal, 2022).

Penjelasan tentang teknologi *blockchain* ialah suatu metode untuk penyimpanan data, yang mana terdiri atas kumpulan *node – node* yang saling terkoneksi pada jaringan *blockchain* dan sifatnya terdesentralisasi. Kemudian akan terdapat kumpulan *record* atau catatan transaksi digital data yang berbentuk blok dan saling berkaitan sehingga akan terlihat seperti bentuk rantai blok di dalamnya. Ketika adanya kegiatan transaksi maka akan ditandai menurut waktu prosesnya terjadi kemudian diubah ke dalam blok yang mana dengan hash kriptografiknya akan mengidentifikasi masing – masing dari blok tersebut (Rika Widianita, 2023)



Gambar 2. 1 Cara kerja *Blockchain*

Proses kerja *blockchain* dimulai ketika seorang pengguna melakukan transaksi, misalnya mengirim uang ke pihak lain. Setelah transaksi dilakukan, data tersebut dikonversi menjadi bentuk blok dan dikirimkan ke jaringan komputer dalam sistem *blockchain*. Selanjutnya, jaringan komputer yang terdistribusi akan melakukan validasi untuk memastikan keabsahan data dan menyetujui permintaan transaksi. Setelah diverifikasi, transaksi ini diberi hash, yaitu sebuah identitas unik yang menghubungkan blok tersebut dengan blok sebelumnya dalam rantai *blockchain*. Blok yang telah tervalidasi kemudian bergabung dengan rantai blok yang sudah ada, membentuk catatan permanen yang berisi riwayat aktivitas transaksi. Akhirnya, transaksi dianggap berhasil dan data yang telah diverifikasi tersimpan secara aman di dalam *blockchain*, memastikan integritas dan keamanan informasi.

2.2.2 OCR *Deep Learning*

Dalam proyek kali ini, peneliti tidak hanya menggunakan OCR biasa, tetapi dilengkapi dengan *deep learning,* yaitu EasyOCR. OCR *Deep Learning* ini bertujuan untuk meningkatkan akurasi dalam membaca teks dari citra

digital. Dengan OCR *Deep Learning* ini, sistem akan lebih fleksibel dalam mengenali karakter dan akan bekerja lebih baik daripada OCR tradisional. OCR merupakan teknologi untuk mengekstrak teks dari sebuah gambar digital (Pratomo dkk., 2022).

Deep Learning dalam OCR memanfaatkan jaringan saraf tiruan (Artificial Neural Networks/ANN), terutama Convolutional Neural Networks (CNN) dan Recurrent Neural Networks (RNN). CNN digunakan untuk mengekstrak fitur visual dari citra teks, seperti bentuk huruf dan pola karakter, CNN juga memiliki kemampuan untuk mengekstrak fitur-fitur penting dan membangun representasi yang kuat, sehingga angat cocok untuk tugas pengenalan karakter(Swasono dkk., 2024)

sedangkan RNN, khususnya Long Short-Term Memory (LSTM), digunakan untuk memproses urutan karakter dalam teks. Kombinasi CNN dan RNN dalam model OCR, seperti arsitektur CRNN (Convolutional Recurrent Neural Network), telah terbukti meningkatkan akurasi dalam mengenali teks yang kompleks, termasuk tulisan tangan dan karakter dari berbagai bahasa. EasyOCR sebenarnya adalah pake python yang menampung Pytorch sebagai penanganan backend. EasyOCR mendukung 42 lebih bahasa untuk tujuan deteksi. EasyOCR dibuat oleh perusahaan bernama Jaided Al Company(Hanan & Jihaannuriy, 2022)

Cara kerja OCR AI dalam proyek ini ketika citra digital di unggah ke dalam sistem dan diolah di tahap *prepocessing dataset*, selanjutnya Easy OCR akan digunakan untuk mengenali dan mengekstrak teks dari gambar sertifikat. Hasil dari OCR AI tersebut akan berupa list daftar yang berisi teks yang dikenali dari gambar digital tersebut.

2.2.3 Keamanan Citra Digital

Kemanan citra digital merupakan upaya untuk melindungi keaslian, kerahasiaan data gambar, maupun untuk melindungi integritas. Citra digital yang bersifat pribadi dan rahasia sangat rentan terhadap peyadapan oleh pihak-pihak yang tidak bertanggung jawab. Terutama bila didistribusikan melalui jaringan internet seperti pada aplikasi berbasis chatting facebook, whatsapp dan media e-mail. Karena citra digital masih berupa citra yang dapat

dikenali dan dapat dimanfaatkan oleh pihak pemanipulasi untuk keuntungan pribadi sehingga merugikan pihak yang memiliki akses terhadap data citra(Azanuddin et al., 2022)

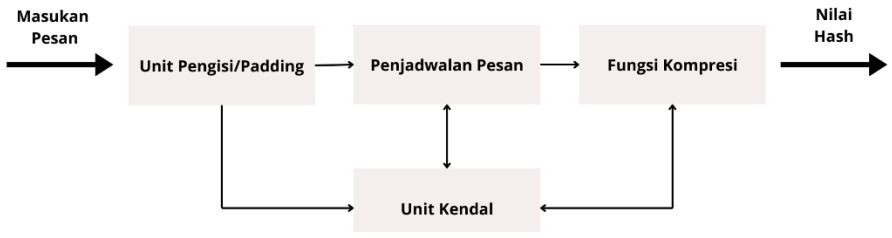
Tabel 2. 1 Contoh Teknik Keamanan

Teknik Keamanan	**Deskripsi**	**Contoh Aplikasi**
Kriptografi	Kriptografi adalah ilmu yang mempelajari tentang cara menjaga keamanan suatu pesan atau informasi. Pesan atau informasi dapat dikategorikan ke dalam dua jenis, yaitu pesan yang dapat dibaca dengan mudah (plaintext) dan pesan yang tidak mudah dibaca (ciphertext) (Poetro et al., 2010).	Enkripsi gambar menggunakan algoritma seperti AES untuk menccegah akses tidak sah
Watermarking	Watermarking merupakan Suatu teknik penyembunyian data/informasi rahasia kedalam citra digital baik berupa logo, teks ataupun citra (Syahdilan & Prawira, 2024).	Menambahkan logo atau teks tersembunyi dalam gambar untuk memverifikasi keaslian gambar
Stenografi	Steganografi adalah ilmu menyembunyikan teks pada media lain yang telah ada sedemikian sehingga teks yang tersembunyi menyatu dengan media itu. Media tempat penyembunyian pesan tersembunyi dapat berupa media teks, gambar, audio atau video (Satria & Antares, 2022).	Menyembunyikan pesan teks atau file lain dalam gambar untuk tujuan komunikasi rahasia

2.2.4 Algoritma SHA-256

SHA (Algoritma keamanan fungsi hash) merupakan algoritma enkripsi fungsi hash yang dapat digunakan untuk menghasilkan penggambaran konsolidasi dari sebuah data teks yang disebut sebuah proses pesan. SHA-256 dan SHA-512 adalah fungsi hash dengan kapasitas terbaru dengan panjang 32 bit dan 64-bit kata secara terpisah. Kedua fungsi hash ini dalam proses matematisnya menggunakan penjumlahan karakter yang berbeda dan ditambah dengan konstanta substansi. Meski demikian, struktur keduanya pada dasarnya tidak jauh berbeda, perbedaannya hanya terletak pada jumlah putaran saja sulit untuk membalikkan nilai *hash* guna mendapatkan data aslinya(Zufria dkk.,)

SHA(SecurehashAlgorithm) adalah salah satu algoritma hash yang relatif masih baru. Algoritma ini dirancang oleh The National Institute of Standards and Technology (NIST) pada tahun 2002. SHA – 256 menghasilkan *message digest* dengan panjang 256 bits. SHA – 256 tergolong aman karena didesain sedemikian rupa sehingga tidak memungkinkan mendapatkan pesan yang berhubungan dengan message digest yang sama. Seperti pada contoh kasus dokumen citra digital hasil pemindaian dari ijazah dan transkrip nilai. Proses untuk menghasilkan message *digest* pada algoritma ini meliputi lima tahapan(Nainggolan, 2022)



Gambar 2. 2 Arsitektur sederhana SHA-256

Gambar tersebut merupakan alur dari proses *hashing* dalam sebuah algoritma SHA-256.

1. Masukan Pesan

   Data atau pesan awal yang akan diubah menjadi nilai hash dimasukkan ke dalam sistem.

2. Unit Pengisi/Padding

   Pesan yang dimasukkan mungkin tidak memiliki panjang yang sesuai dengan blok yang diperlukan oleh algoritma *hashing*. Oleh karena itu, unit ini menambahkan padding (data tambahan) agar pesan memiliki panjang yang sesuai untuk diproses lebih lanjut.

3. Penjadwalan Pesan

   Setelah dilakukan padding, pesan dijadwalkan dalam blok-blok kecil untuk diproses secara berurutan. Blok-blok ini akan digunakan dalam berbagai tahap perhitungan hash.

4. Fungsi Kompresi

   Fungsi ini melakukan serangkaian operasi matematika dan logika terhadap blok pesan yang telah dijadwalkan. Ini adalah bagian inti dari algoritma hashing, di mana data diproses menjadi bentuk unik dan tidak dapat dibalik.

5. Unit Kendali

   Berfungsi sebagai pengatur seluruh proses hashing, memastikan setiap langkah dilakukan dalam urutan yang benar. Mengontrol komunikasi antara unit pengisi, penjadwalan pesan, dan fungsi kompresi.

6. Nilai Hash

   Hasil akhir dari proses hashing berupa nilai hash yang unik. Nilai ini bersifat tetap untuk input yang sama dan berubah secara signifikan jika ada sedikit perubahan dalam input.

2.2.5 *Smart contract* Remix IDE

Gambar 2. 3 Remix IDE

Smart contract adalah program komputer yang dijalankan di dalam *Blockchain* untuk mengeksekusi transaksi secara otomatis berdasarkan kondisi yang telah ditentukan sebelumnya. *Smart contract* juga dijelaskan sebagai seperangkat aturan untuk memfasilitasi transfer mata uang atau aset digital antar pihak dalam kondisi tertentu secara digital. Smart contract adalah program komputer aman yang memiliki verifikasi diri, eksekusi mandiri, dan sifat tahan akan kerusakan. Smart contract digunakan untuk pertukaran nilai tanpa perlu pihak ketiga. Smart contract membantu kita menukar uang, properti, saham, atau apa pun yang berharga secara transparan, dan menghindari layanan perantara. Smart contract berjalan di Mesin Virtual Ethereum (EVM) (Rochmatullah, 2022)

Smart contract pada Ethereum ditulis dalam bahasa pemrograman *Solidity*, dan dijalankan di dalam lingkungan *virtual machine* yang disebut Ethereum Virtual Machine (EVM). *Smart contract* pada *blockchain* dapat digunakan untuk berbagai jenis aplikasi, seperti perbankan, asuransi, dan logistik. Salah satu contoh penggunaan *smart contract* adalah dalam industri asuransi, di mana *smart contract* dapat digunakan untuk mengeksekusi klaim secara otomatis berdasarkan kondisi tertentu, seperti cuaca yang buruk atau kejadian bencana alam(Rika Widianita, 2023)

Dalam upaya mengurangi interaksi secara langsung, *smart contract* mulai digunakan dalam kegiatan transaksi secara elektronik. *Smart contract*

yang pertama kali dikenalkan oleh Nick Szabo merupakan kumpulan kode yang disimpan dan diproses dalam sistem buku besar terdistribusi (Distributed Ledger Technology/DLT) komputer yang diprogram untuk berjalan secara otomatis sesuai dengan kondisi tertentu yang telah ditentukan sebelumnya. Penerapan *blockchain-smart contract* tersebut tidak terbatas pada kegiatan perdagangan, melainkan juga dalam bidang perasuransian (insurance), crowd funding, hingga penyediaan jasa. *Smart contract* telah diterapkan dalam kegiatan transaksi elektronik di beberapa negara, seperti pada Quube di Singapura, Elinext dari Perancis, (Kadly dkk., 2021)

2.2.6 MetaMask

Gambar 2. 4 Metamask

Konfigurasi metamask merupakan tahapan penting dalam perancangan aplikasi point of saleberbasis *blockchain*. Metamask berperan sebagai penghubung antara aplikasi dan *blockchain*untuk dapat berinteraksi dengan smart contractdan melakukan transaksi menggunakan crypto wallet. Konfigurasi metamask melibatkan penambahan alamat smart di Ganache(Yogiyanti & Suartana, 2024)

Selain sebagai dompet *cryptocurrency*, metamask berguna untuk menghubungkan pengguna dengan aplikasi desentralisasi Ethereum. Dengan adanya metamask, membuat proses transaksi pada aplikasi terdesentralisasi menjadi lebih aman. Sebelumnya aplikasi terdesentralisasi harus memberikan *private key* ke *cryptocurrency wallet*, namun dengan adanya metamask aplikasi terdesentralisasi informasi dokumen dan menyimpannya ke sistem *blockchain* (Timothy Harlian dkk., 2022).

Dalam proyek ini, MetaMask membantu memastikan bahwa hanya akun yang memiliki izin yang dapat berinteraksi dengan *Smart contract* , sehingga

keamanan data yang tersimpan di *blockchain* tetap terjaga. Selain itu, MetaMask juga digunakan untuk melakukan transaksi di jaringan Ethereum jika nantinya sistem ini diterapkan di lingkungan *blockchain* yang sebenarnya, di mana setiap transaksi akan membutuhkan gas fee dalam bentuk Ethereum.

2.2.7 Ganache

Gambar 2. 5 Ganache

Ganache adalah sebuah *simulator blockchain* Ethereum yang beroperasi secara lokal di computer. Ganache mengambil prinsip dasar dari sistem terdesentralisasi, di mana setiap informasi yang disimpan dalam jaringan *blockchain* akan didistribusikan ke semua partisipan jaringan. Dalam hal keamanan, tidak ada satu entitas pun yang memiliki kendali mutlak atas data atau transaksi yang terjadi di jaringan *blockchain*. Setiap *node* atau validator dalam jaringan memiliki salinan data yang identik. Dengan demikian, teknologi *blockchain* memungkinkan terjadinya transaksi yang aman dan efisien tanpa harus bergantung pada suatu organisasi atau entitas berpengaruh yang mengatur aliran transaksi data(Yogiyanti & Suartana, 2024)

Penggunaan *smart contract* memastikan bahwa transaksi dilakukan secara otomatis dan sesuai dengan aturan yang telah ditetapkan. Ganache menyediakan lingkungan uji yang aman untuk pengembangan, sementara metamask memfasilitasi interaksi pengguna dengan blockchain, memastikan bahwa setiap transaksi diverifikasi dan aman. Semua komponen ini berintegrasi untuk memberikan solusi yang efisien dan aman bagi pengguna dalam melakukan transaksi di aplikasi point of saleberbasis blockchain(Yogiyanti & Suartana, 2024)

BAB III
METODE PENELITIAN

3.1 Deskripsi Sistem

Dalam penelitian ini, sistem yang dikembangkan berupa web yang dirancang untuk memastikan keaslian sertifikat digital menggunakan algoritma SHA-256 dan dilengkapi dengan teknologi *blockchain*. Sistem ini dibangun dengan bahasa pemrograman Python, di mana Flask digunakan sebagai *framework backend* untuk menangani logika aplikasi serta pengelolaan data. Sementara itu, antarmuka pengguna dikembangkan menggunakan HTML, CSS, dan JavaScript, sehingga menghasilkan tampilan yang interaktif dan responsif.

Agar sistem dapat berjalan secara lokal, digunakan XAMPP sebagai server untuk mengelola database dan memproses data sertifikat. Proses verifikasi keaslian sertifikat memanfaatkan teknologi OCR berbasis AI, yang berfungsi mengekstraksi teks dari sertifikat secara otomatis. Setelah teks diperoleh, sistem menerapkan algoritma SHA-256 untuk mengubah teks menjadi *hash* unik, yang kemudian dibandingkan dengan *hash* yang telah tersimpan sebelumnya. Data *hash* ini selanjutnya disimpan dan diverifikasi menggunakan *blockchain* Ethereum lokal yang dioperasikan melalui Ganache, guna memastikan keamanan serta integritas data sertifikat yang telah diverifikasi.

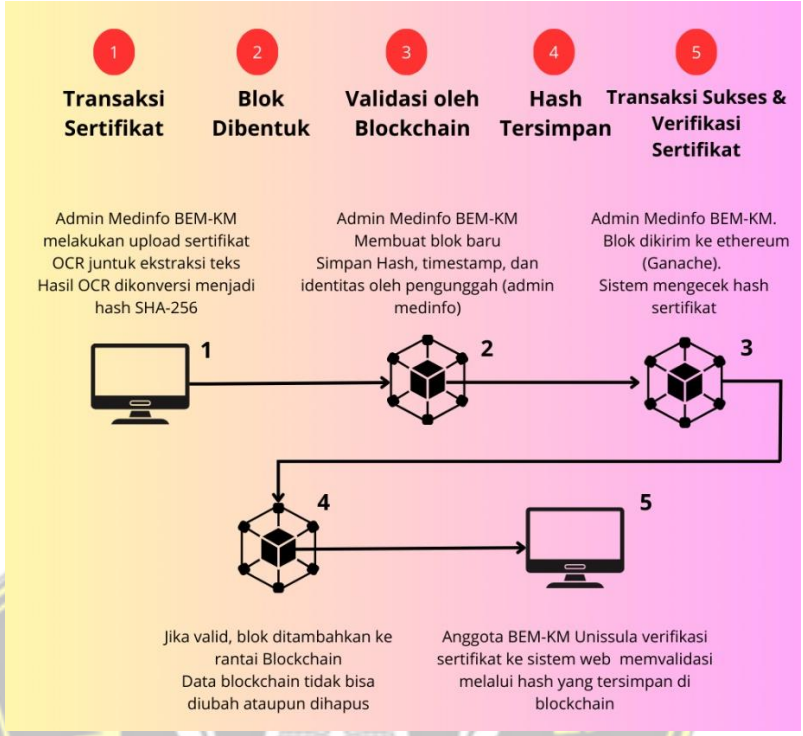
3.2 Studi Literatur

Studi literatur mencakup e-book, artikel, dan jurnal tentang OCR Deep Learning, *hashing* menggunakan SHA-256, *Blockchain* untuk merumuskan masalah dan solusi sistem pendeteksi sertifikat digital.

3.3 Rancang Alur Model

Pada tahap ini peneliti akan merancang alur kerja dari sistem yang akan dibuat. Untuk merepresentasikan alur kerja sistem, peneliti akan membuatnya

dalam sebuah alur kerja *blockchain* dalam sistem verifikasi sertifikat digital, *flowchart* sederhana berupa *flowchart* admin dan *flowchart* verifikasi.

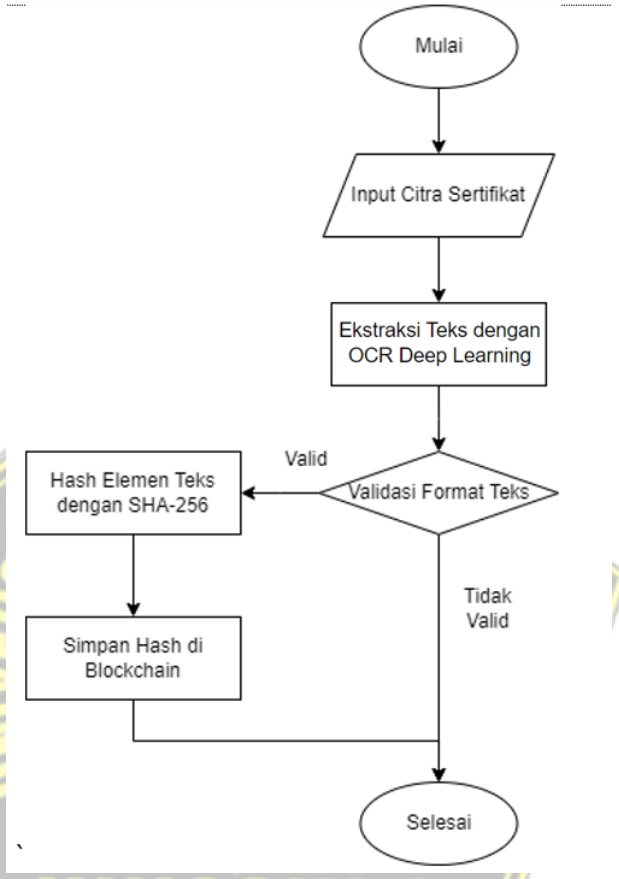


Gambar 3. 1 Alur kerja *blockchain*

Gambar 3.1 merupakan alur kerja *blockchain* yang dilakukan oleh admin untuk menginput data sertifikat digital setelah melalui tahap *preprocessing* data. Pada tahap awal, sertifikat yang diunggah oleh Admin Medinfo BEM-KM akan diproses menggunakan EasyOCR untuk mengekstraksi teks yang terdapat di dalamnya. Setelah proses OCR selesai, sistem akan melakukan *hashing* menggunakan algoritma SHA-256 terhadap dua elemen utama, yaitu gambar sertifikat dan teks hasil OCR. Proses *hashing* ini bertujuan untuk memastikan integritas dan keamanan data sertifikat.

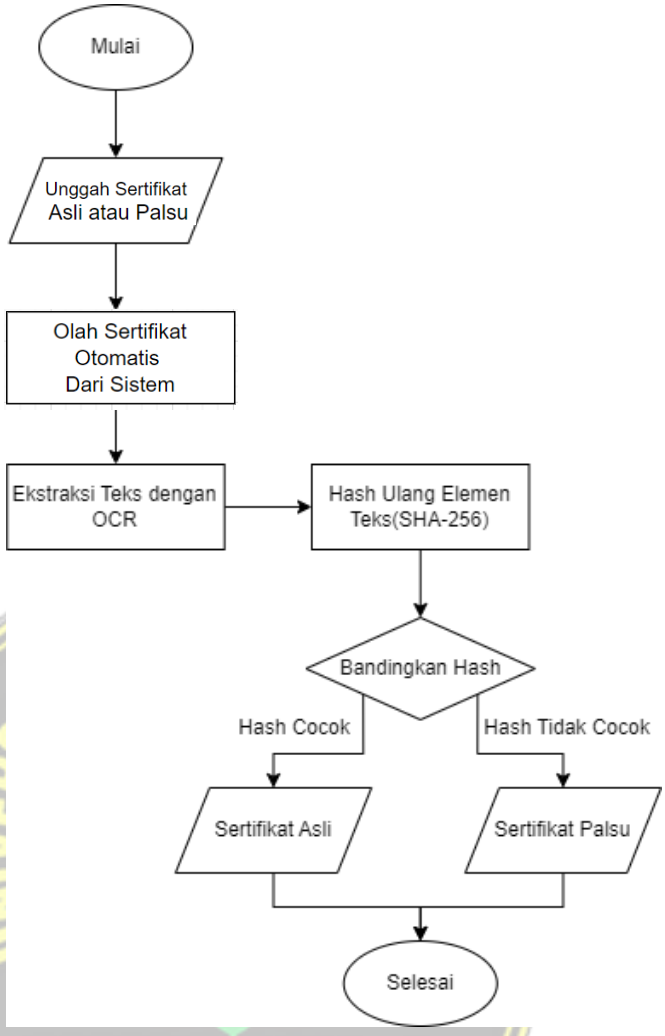
Selanjutnya, hasil *hashing* akan disimpan di *database* serta dicatat dalam *blockchain* Ethereum (Ganache). Sistem akan membentuk blok baru yang berisi *hash* sertifikat, timestamp, serta identitas pengunggah sebelum divalidasi oleh *blockchain*. Jika valid, blok tersebut akan ditambahkan ke dalam rantai *blockchain*, di mana data yang tersimpan tidak dapat diubah maupun dihapus. Pada tahap akhir, anggota BEM-KM Unissula dapat melakukan verifikasi sertifikat melalui sistem web dengan mencocokkan *hash* yang tersimpan di *blockchain*. Jika *hash* yang dihasilkan dari sertifikat yang

diunggah sesuai dengan *hash* yang tersimpan, maka sertifikat dinyatakan valid atau asli, sehingga dapat diverifikasi dengan aman dan transparan.



Gambar 3. 2 *Flowchart* Alur Sistem Admin

Gambar 3.2 merupakan diagram alur sistem deteksi admin untuk menginput data sertifikat digital yang sudah di melewati *preprocessing* data. Sertifikat tersebut akan di OCR menggunakan EasyOCR untuk menghasilkan teks OCR, lalu sertifikat dan teks hasil OCR sertifikat di*hashing* menggunakan SHA-256. Kemudian hasil *hashing* disimpan di *database* dan *blockchain*.



Gambar 3. 3 *Flowchart* Sistem Verifikasi

Gambar 3.3 adalah *flowchart* alur sistem verifikasi sertifikat. Proses dimulai dengan menginput sertifikat asli maupun sertifikat yang sudah dimanipulasi. Lalu sertifikat tersebut akan diolah otomatis dari sistem untuk di *greyscale* dan di *resize*. Setelah itu akan di OCR *Deep Learning* untuk menghasilkan teks OCR dan akan di *hashing*. Setelah sertifikat tersebut sudah menghasilkan *hash* gambar dan *hash* teks, akan dibandingkan dengan *hash* yang sudah tersimpan di *blockchain* maupun di *database.* Apabila *hash* cocok maka sertifikat tersebut asli, dan apabila *hash* tidak cocok, maka sertifikat tersebut palsu.

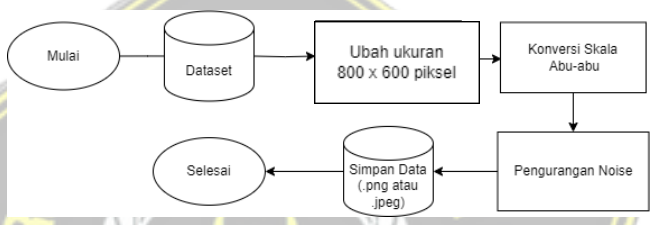
3.4 Tahapan Perancangan Model

3.4.1 Pengumpulan *Dataset*

Pembuatan program pada sistem ini diawali dengan mengumpulkan *dataset* yang akan diolah. Dimana terdapat dataset berupa sertifikat digital asli yang berjumlah 258 dan dataset sertifikat yang sudah dimanipulasikan berjumlah 25 sertifikat palsu.

3.4.2 *Preprocessing* Dataset

Pada tahap ini adalah proses melakukan olah data, dimana sertifikat digital asli akan diolah agar lebih mudah dikenali oleh OCR AI untuk proses ekstraksi teks.



Gambar 3. 4 Alur *preprocessing* dataset

Gambar diatas merupakan alur *prepocesing dataset.* Dalam proyek verifikasi sertifikat ini, *preprocessing* data merupakan tahap awal yang bertujuan untuk memastikan kualitas gambar sertifikat sebelum diproses lebih lanjut oleh sistem. Proses ini dilakukan untuk meningkatkan akurasi ekstraksi teks menggunakan OCR *Deep Learning* dan menjaga konsistensi hasil *hash*ing SHA-256. *Preprocessing* diterapkan dalam dua tahap utama, yaitu saat admin mengunggah sertifikat ke sistem dan ketika pengguna melakukan verifikasi sertifikat.

Saat sertifikat baru dimasukkan oleh admin, *preprocessing* memastikan gambar memiliki ukuran dan format yang seragam agar hasil OCR lebih optimal. Begitu pula saat pengguna mengunggah sertifikat untuk diuji keasliannya, *preprocessing* kembali diterapkan agar kondisi gambar sesuai dengan dataset yang telah tersimpan, sehingga proses perbandingan *hash* tetap akurat. Tahapan *preprocessing* dimulai dengan mengubah ukuran gambar menjadi 800 x 600 piksel agar resolusi lebih jelas. Setelah itu, gambar dikonversi ke skala abu-abu untuk meningkatkan kontras dan mengurangi gangguan warna. Selanjutnya, dilakukan proses pengurangan *noise* guna

menghilangkan elemen-elemen yang dapat mengganggu pembacaan teks oleh OCR. Setelah semua tahap ini selesai, gambar sertifikat disimpan dalam format PNG atau JPEG untuk kemudian digunakan dalam proses verifikasi lebih lanjut.

3.4.3 Proses OCR *Deep Learning*

Dalam proyek ini, sistem OCR berbasis *deep learning* menggunakan EasyOCR, yang menerapkan pendekatan Convolutional Recurrent Neural Network (CRNN) untuk meningkatkan akurasi pengenalan teks dari citra digital. Metode ini menggabungkan dua arsitektur utama, yaitu Convolutional Neural Network (CNN) untuk mengekstraksi fitur visual dari gambar dan Long Short-Term Memory (LSTM) sebagai bagian dari Recurrent Neural Network (RNN) untuk mengenali serta memahami urutan karakter dalam teks yang telah terdeteksi.

Proses dimulai dengan deteksi area teks, di mana CNN menganalisis gambar untuk mengidentifikasi lokasi yang mengandung teks, bahkan jika ada variasi gaya tulisan atau gangguan visual. Setelah itu, bagian ekstraksi karakter dilakukan dengan memanfaatkan LSTM, yang memiliki kemampuan dalam memahami hubungan antar karakter dalam satu kata atau kalimat. LSTM bekerja dengan mempertimbangkan konteks karakter sebelumnya dan berikutnya, sehingga dapat membedakan karakter yang memiliki bentuk serupa, seperti angka "0" dan huruf "O", atau huruf "l" dan angka "1" dengan lebih akurat.

Gambar 3. 5 Proses AI dalam OCR

Pada gambar diatas adalah bukti penerapan *Deep Learning* dalam sistem ini dapat dilihat dari beberapa aspek. Pada tahap pertama, model mampu mendeteksi area teks pada gambar sertifikat, yang ditandai dengan bounding box berwarna hijau sebagaimana terlihat pada hasil pemrosesan OCR. Proses ini menunjukkan bahwa sistem berbasis *Deep Learning* berhasil mengenali lokasi teks dalam gambar sertifikat secara otomatis. Selanjutnya, setelah teks diekstraksi, model mengubahnya menjadi string yang dapat dibandingkan dengan data yang telah tersimpan sebelumnya.

Hasil teks ini kemudian diolah lebih lanjut dengan algoritma SHA-256 *hash*ing, sehingga setiap sertifikat akan memiliki identitas unik dalam bentuk *hash*. *Hash* ini disimpan di database dan *blockchain* untuk memastikan keaslian sertifikat. Ketika pengguna melakukan verifikasi, sistem akan kembali menggunakan OCR berbasis *Deep Learning* untuk membaca teks dari sertifikat yang diunggah, lalu menghasilkan *hash* baru yang dibandingkan dengan *hash* yang telah tersimpan. Jika hasilnya cocok, sertifikat dikategorikan sebagai asli, sebaliknya, jika berbeda, maka dianggap tidak valid atau telah dimodifikasi. Dengan penggunaan metode ini, sistem mampu meningkatkan akurasi dalam membaca teks sertifikat yang memiliki variasi desain, warna, ukuran font, dan tingkat *noise* yang berbeda, memastikan bahwa proses verifikasi berjalan lebih efektif dan aman.

3.4.4 *Hashing* SHA-256

Dalam proyek ini, proses *hash*ing menggunakan algoritma SHA-256 berperan penting dalam menjaga keamanan dan integritas data sertifikat digital. Tahapan *hash*ing dimulai dengan mengolah gambar sertifikat menggunakan teknologi OCR berbasis AI untuk mengekstraksi teks yang terkandung di dalamnya. Setelah teks berhasil diperoleh, sistem menerapkan algoritma SHA-256 untuk mengubah teks tersebut menjadi sebuah nilai *hash* unik yang terdiri dari 64 karakter heksadesimal. Selain itu, sistem juga melakukan *hash*ing terhadap gambar sertifikat setelah melalui proses *grayscale* dan *resize*, guna memastikan bahwa setiap sertifikat memiliki identitas digital yang tetap dan tidak dapat diubah.

Hasil *hash*ing ini kemudian dibandingkan dengan data *hash* yang telah tersimpan sebelumnya di dalam database MySQL dan *blockchain* Ethereum (Ganache). Jika *hash* yang dihasilkan sesuai dengan *hash* yang tersimpan, maka sertifikat dianggap valid dan asli. Dengan menggunakan *blockchain*, setiap *hash* yang tersimpan menjadi lebih aman dan transparan, karena data tidak dapat dimanipulasi atau diubah secara sepihak. Proses ini memastikan bahwa sertifikat yang diverifikasi benar-benar otentik, serta mencegah adanya pemalsuan atau perubahan data yang tidak sah.

3.4.5 Proses Simpan *Hash* ke *Database*

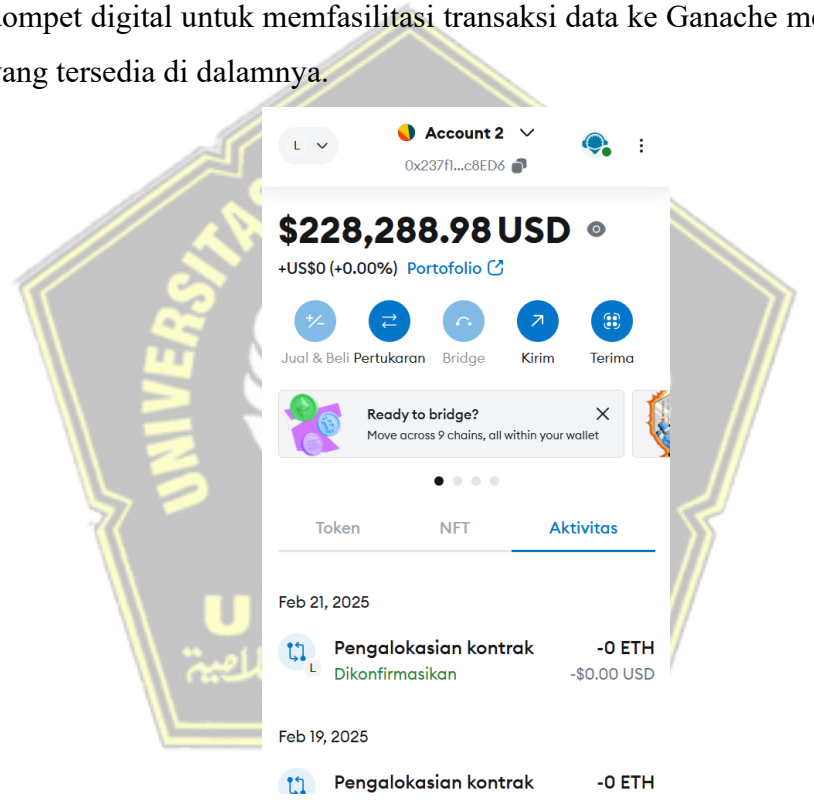
Proses penyimpanan *hash* ke dalam database dilakukan melalui beberapa langkah sistematis untuk memastikan keakuratan dan keamanan data. Pertama, setelah gambar sertifikat diunggah, sistem akan memprosesnya dengan metode OCR berbasis AI untuk mengekstrak teks yang terdapat pada sertifikat. Hasil teks tersebut kemudian diubah menjadi *hash* menggunakan algoritma SHA-256, yang menghasilkan nilai *hash* unik berdasarkan konten sertifikat. Selain itu, gambar sertifikat juga diproses dengan *hash*ing, sehingga diperoleh dua *hash* utama, yaitu *hash* gambar dan *hash* teks hasil OCR.

Setelah proses *hash*ing selesai, sistem akan menyimpan kedua *hash* tersebut ke dalam database MySQL yang dijalankan melalui XAMPP. Penyimpanan dilakukan tanpa menghapus *hash* sebelumnya, sehingga setiap data yang telah tersimpan tetap terdokumentasi dengan baik untuk keperluan

verifikasi di masa mendatang. Database ini menjadi pusat penyimpanan yang digunakan untuk membandingkan hasil *hash* saat proses validasi sertifikat berlangsung.

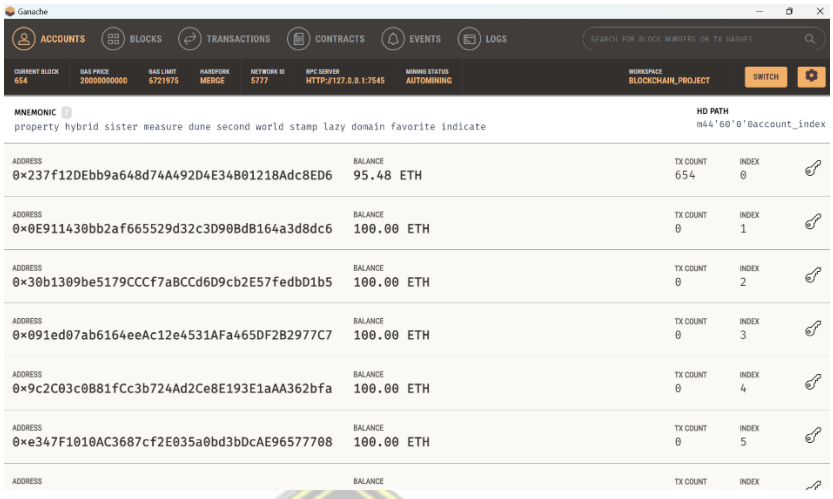
3.4.6 Proses Simpan *Hash* ke *Blockchain*

Tahap berikutnya adalah menyimpan *hash* gambar dan *hash* teks sertifikat ke dalam *blockchain* Ethereum (Ganache). Namun, sebelum proses penyimpanan *hash* dilakukan, diperlukan dompet digital untuk melakukan transaksi ke akun Ganache. Dalam hal ini, MetaMask digunakan sebagai dompet digital untuk memfasilitasi transaksi data ke Ganache melalui alamat yang tersedia di dalamnya.



Gambar 3. 6 Akun dompet digital (MetaMask)

Gambar 3.11 adalah tampilan dompet digital yang akan digunakan sebagai tempat pembayaran transaksi ke alamat akun Ethereum (Ganache). Saldo tersebut di dapatkan ketika sudah menyambungkan MetaMask dengan alamat akun dan memasukan kunci atau *private key* dari salah satu akun di Ganache.



Gambar diatas merupakan tampilan dari akun Ganache yang akan digunakan untuk tempat menyimpan *hash* dari sertifikat.

BAB IV
HASIL DAN ANALISIS PENELITIAN

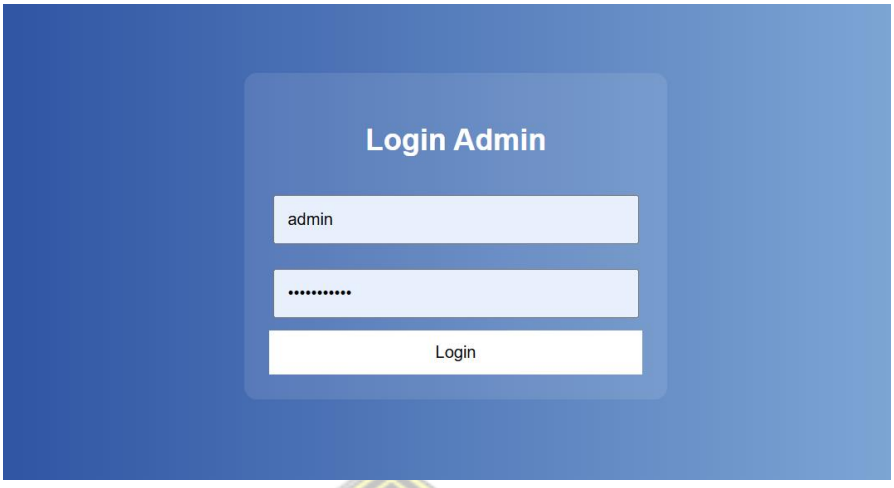
4.1 Hasil dan Analisis

Sistem yang dikembangkan berupa web yang memiliki tujuan untuk memverifikasi keaslian sertifikat digital menggunakan OCR *Deep Learning*, SHA-256 , dan *blockchain* Ethereum (Ganache). Sistem ini memiliki dua komponen utama, yaitu halaman admin sebagai tempat untuk input dan menyimpan sertifikat ke *database* dan *blockchain,* dan halaman verifikasi sebagai tempat untuk memeriksa apakah sertifikat yang di unggah asli atau sudah dimanipulasi (palsu), dengan membandingkan *hash* gambar dan *hash* teks hasil OCR terhadap *database* dan *blockchain*.

4.1.1 Pengujian Unggah dan Penyimpanan Sertifikat

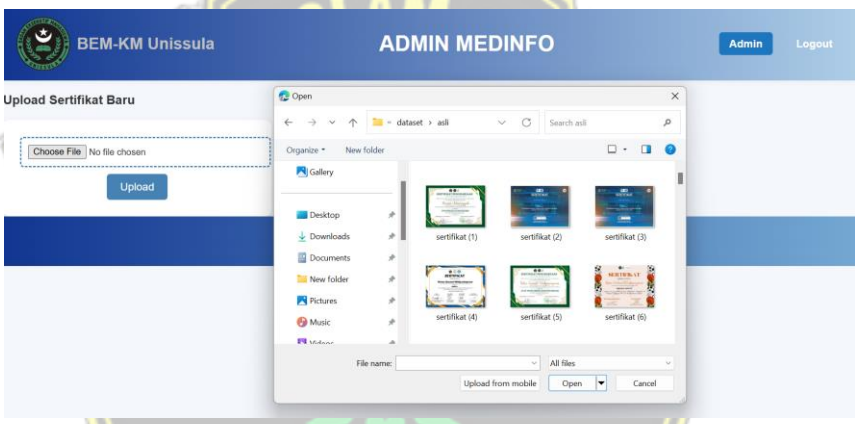
Gambar 4. 1 Tampilan *landing page*

Gambar 4.1 adalah tampilan *landing page*, lalu admin klik tombol "admin" untuk memulai uji *input* data lalu menyimpannya di *database* dan *blockchain* di pojok kiri atas.



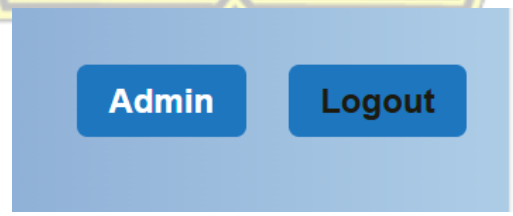
Gambar 4. 2 Tampilan *login* admin

Gambar 4.2 merupakan tampilan dari *login admin.*



Gambar 4. 3 Tampilan admin *input* sertifikat digital

Gambar 4.3 merupakan tampilan input pada halaman admin untuk diupload dan disimpan di *database* dan *blockchain.*

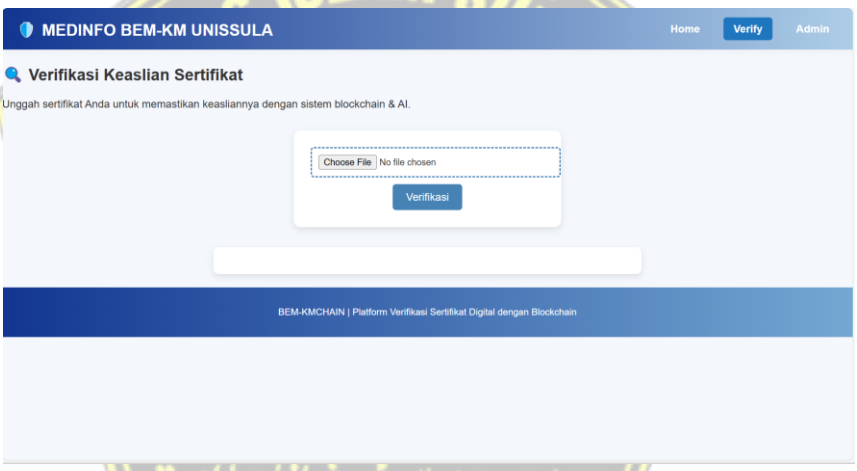


Gambar 4. 4 Tampilan *logout* pada admin *page*

Gambar 4.4 adalah tampilan untuk *logout* pada admin yang terdapat di pojok kiri atas web. Ketika diklik makan akan kembali ke halaman *landing page.*

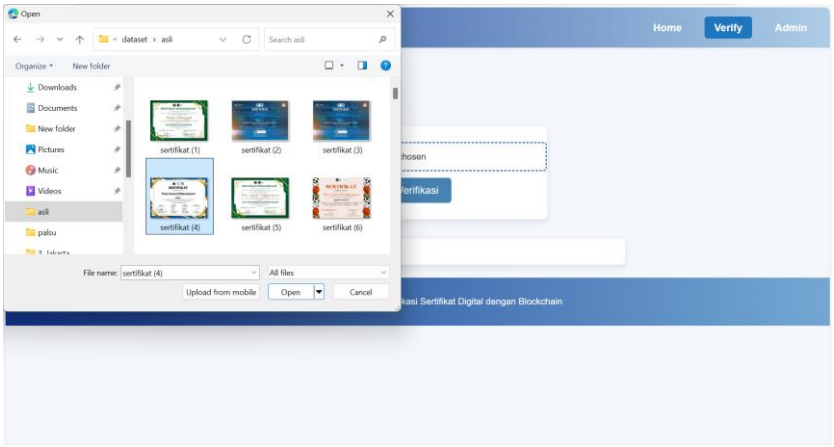
Gambar 4. 5 Tampilan *landing page*

Gambar 4.5 adalah tampilan *landing page*, lalu klik "verifikasi" untuk beralih ke halaman verifikasi sertifikat digital



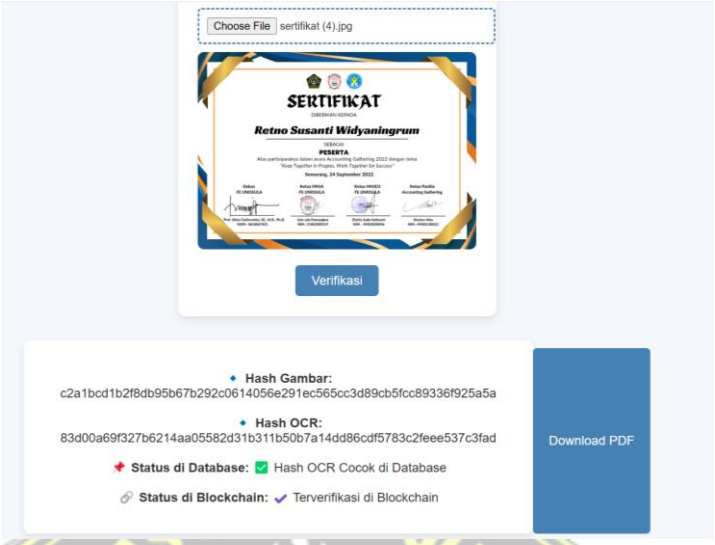
Gambar 4. 6 Halaman Verifikasi sertifikat digital

Gambar 4.6 adalah tampilan pada halaman untuk verifikasi keaslian sertifikat.



Gambar 4. 7 Tampilan memilih dataset asli untuk diverifikasi

Gambar 4.7 merupakan tampilan untuk memilih dataset asli untuk menguji sertifikat digital asli yang akan diuji. Lalu klik tombol verifikasi.

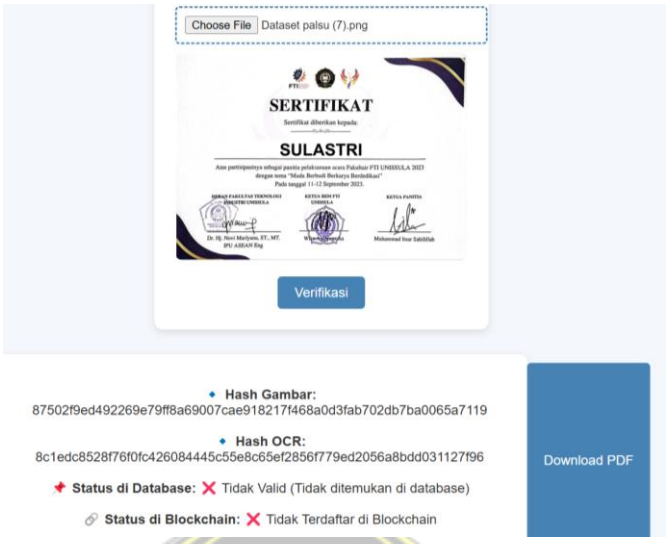


Gambar 4. 8 Tampilan hasil uji coba sertifikat

Gambar 4.8 merupakan hasil uji sertifikat digital dan hasilnya sertifikat asli, karena *hash* terdaftar di *blockchain* dan *database*.

Gambar 4. 9 Tampilan memilih dataset asli untuk diverifikasi

Gambar 4.9 merupakan tampilan untuk memilih dataset palsu untuk menguji asli atau palsu sertifikat digital yang akan diuji



Gambar 4. 10 Tampilan hasil uji coba sertifikat

Gambar 4.1 merupakan hasil uji sertifikat digital dan hasilnya sertifikat palsu, karena *hash* tidak terdaftar di *blockchain* dan *database*.

4.1.2 Analisis Akurasi Dataset

Pada penelitian ini, dilakukan pengujian untuk mengevaluasi akurasi sistem dalam memverifikasi keaslian sertifikat menggunakan metode *hashing* SHA-256 dan teknologi OCR berbasis AI. Pengujian dilakukan dengan membandingkan hasil *hashing* dari sertifikat asli dan palsu terhadap data yang telah tersimpan di database dan *blockchain*.

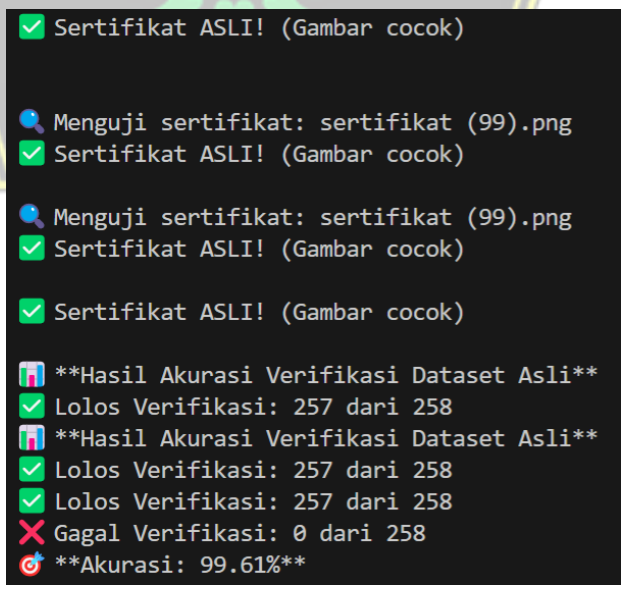
$$\text{Akurasi} = \left(\frac{\text{Jumlah Lolos Verifikasi}}{\text{Total Sertifikat Uji}} \right) \times 100\%$$

Gambar 4. 11 Rumus menghitung akurasi

Gambar diatas merupakan rumus untuk menghitung akurasi dengan membandingkan jumlah sertifikat yang berhasil diverifikasi dengan total sertifikat yang diuji.

Gambar 4. 12 Kumpulan sertifikat asli

Gambar diatas merupakan kumpulan dari semua dataset asli yang berjumlah 258 sertifitikat digital, gambar tersebut akan diuji akurasinya untuk mengetahui ada berapa sertifikat yang bisa diuji sesuai dengan hasil yang diharapkan yaitu sertifikat asli dan ada berapa sertifikat asli yang terdeteksi tidak terverifikasi.



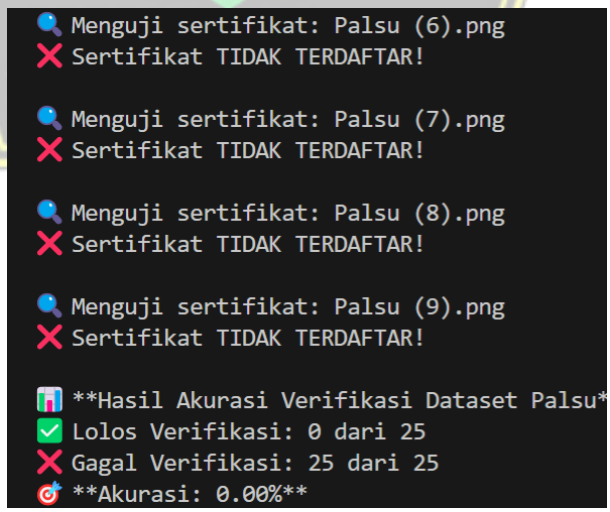
Gambar 4. 13 Hasil analisis akurasi

Gambar diatas merupakan hasil dari analisis akurasi menggunakan dataset asli. Hasil pengujian menunjukkan bahwa sistem memiliki tingkat

akurasi yang sangat tinggi dalam mengenali sertifikat asli, dengan tingkat keberhasilan 99,61% dari 258 sertifikat yang diuji. Sebanyak 257 sertifikat berhasil diverifikasi sebagai dokumen asli, sedangkan 1 sertifikat mengalami kesalahan verifikasi.

Gambar 4. 14 Kumpulan dataset palsu

Gambar diatas merupakan kumpulan dari semua dataset palsu yang berjumlah 25 sertifitikat digital, manipulasi tersebut dengan mengubah nama dari sertifikat asli. Sertifikat tersebut akan tersebut akan diuji akurasinya untuk mengetahui ada berapa sertifikat yang bisa diuji sesuai dengan hasil yang diharapkan yaitu tidak terdeteksi.



Gambar 4. 15 Hasil analisis akurasi

Gambar diatas merupakan hasil dari analisis akurasi menggunakan dataset palsu. Saat diuji dengan 25 sertifikat palsu, sistem mampu mengidentifikasi seluruhnya sebagai dokumen yang tidak terdaftar,

menghasilkan tingkat deteksi 100% atau hasil akurasinya adalah 0.00% terhadap sertifikat palsu. Hal ini menunjukkan bahwa metode yang diterapkan dalam penelitian ini efektif dalam mendeteksi keaslian sertifikat dan menghindari pemalsuan.

4.1.3 Hasil Evaluasi Model

Setelah melakukan beberapa pengujian di atas didapatkan hasil sebagai berikut:

A. Interpretasi Hasil

Berdasarkan hasil pengujian, sistem yang dikembangkan telah berhasil melakukan deteksi sertifikat dengan tingkat akurasi yang cukup baik. *Hash* gambar dan *hash* hasil OCR dapat dibandingkan dengan *database* dan *blockchain* untuk menentukan keaslian sertifikat. Jika *hash* gambar cocok, maka sertifikat dianggap asli, sementara ketidaksesuaian menunjukkan kemungkinan sertifikat palsu. Adanya perbedaan pada *hash* OCR meskipun *hash* gambar cocok menunjukkan bahwa teks hasil ekstraksi bisa mengalami variasi, kemungkinan disebabkan oleh kualitas cetakan atau faktor lain.

Dengan demikian, hasil pengujian ini menegaskan bahwa metode *double hashing* yang diterapkan yaitu *hashing* pada gambar dan hasil OCR dapat meningkatkan keandalan sistem dalam menentukan keaslian sertifikat. Pendekatan ini memungkinkan sistem untuk mendeteksi kemungkinan sertifikat palsu tidak hanya dari manipulasi gambar, tetapi juga dari ketidaksesuaian isi teks yang seharusnya sama dengan data yang tersimpan dalam *blockchain*.

B. Faktor yang Mempengaruhi Hasil

Terdapat beberapa faktor yang mempengaruhi hasil deteksi, antara lain:

1. Kualitas gambar sertifikat**:** Gambar dengan resolusi rendah atau buram dapat menyebabkan hasil OCR kurang akurat, sehingga mempengaruhi hasil verifikasi.
2. *Preprocessing* gambar: Teknik yang digunakan dalam *grayscale* dan *resizing* harus konsisten untuk memastikan bahwa *hash* yang dihasilkan tidak berubah

C. Kinerja model OCR: Meskipun AI yang digunakan telah mampu mengekstrak teks dengan cukup baik, ada kemungkinan terjadi kesalahan deteksi akibat jenis font, posisi teks, atau tanda tangan yang mengganggu proses ekstraksi.

D. Kelebihan dan Kekurangan Sistem

Kelebihan:

1. Proses verifikasi lebih cepat karena hanya memerlukan pencocokan *hash*.
2. Kombinasi *hash* gambar dan *hash* OCR memberikan tingkat keamanan lebih tinggi.
3. *Blockchain* digunakan sebagai penyimpanan permanen sehingga data tidak mudah dimanipulasi.

Kekurangan:

1. Jika kualitas gambar buruk, hasil OCR bisa berbeda dan menyebabkan mismatch pada *hash* teks.
2. Sistem belum sepenuhnya mendeteksi ciri khas fisik sertifikat seperti watermark atau tanda tangan secara langsung.

E. Implikasi dan Potensi Pengembangan

Sistem ini memiliki potensi besar untuk diterapkan dalam berbagai institusi yang memerlukan verifikasi dokumen digital. Pengembangannya dapat dilakukan dengan meningkatkan akurasi OCR menggunakan model *Deep Learning* yang lebih canggih atau menambahkan fitur deteksi elemen visual seperti cap dan tanda tangan. Selain itu, integrasi dengan *blockchain* publik dapat meningkatkan transparansi dan keamanan lebih lanjut.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Penelitian ini mengembangkan sistem verifikasi sertifikat digital berbasis *blockchain* dengan menggunakan dua halaman utama, yaitu halaman admin dan halaman verifikasi. Halaman admin berfungsi untuk menginput sertifikat asli, sementara halaman verifikasi digunakan untuk menguji keaslian sertifikat yang diunggah pengguna.

Dalam prosesnya, OCR berbasis AI digunakan untuk mengekstraksi teks dari sertifikat. Teks hasil ekstraksi tersebut kemudian diubah menjadi nilai *hash* menggunakan algoritma SHA-256. Setiap sertifikat akan memiliki nilai *hash* unik yang berfungsi sebagai sidik jari digital, memastikan bahwa sertifikat tersebut tidak dapat dimodifikasi tanpa terdeteksi.

Hasil *hash*ing dari teks OCR serta *hash*ing dari gambar sertifikat disimpan dalam dua sistem penyimpanan: database MySQL dan *blockchain* Ethereum (Ganache). Ketika sebuah sertifikat diuji keasliannya, sistem akan melakukan *hash*ing ulang terhadap teks hasil OCR dan gambar sertifikat yang diunggah. *Hash* yang dihasilkan akan dibandingkan dengan *hash* yang sudah tersimpan di database dan *blockchain*.Jika *hash* yang baru dihasilkan sesuai dengan *hash* yang telah tersimpan, maka sistem akan menyatakan bahwa sertifikat tersebut asli. Sebaliknya, jika terjadi ketidaksesuaian, maka sertifikat dianggap palsu atau telah mengalami perubahan.

Kesimpulan dari penelitian ini menunjukkan bahwa metode verifikasi berbasis *blockchain* dengan metode OCR *Deep Learning* dan algoritma SHA-256 dapat meningkatkan keamanan dan akurasi dalam mendeteksi keaslian sertifikat digital. Sistem ini mampu mencegah pemalsuan sertifikat karena setiap perubahan pada sertifikat akan menghasilkan *hash* yang berbeda, sehingga mudah terdeteksi oleh sistem verifikasi.

5.2 Saran

Beberapa saran untuk pengembangan lebih lanjut :

1. Integrasi *Blockchain* yang Lebih Kuat

   Pada penelitian ini hanya menggunakan *private blockchain* atau jaringan lokal.

2. Pengembangan AI dengan metode tambahan

   Mengoptimalkan OCR AI dalam membaca dan mengektraksi teks. Dengan langkah-langkah ini, diharapkan sistem verifikasi sertifikat lebih siap digunakan di dunia nyata

3. Fitur dalam web

   Pada hasil web admin dan verifikasi sertifikat digital ini masih belum lengkap. Belum termasuk hapus maupun edit data secara langsung di web tersebut.

DAFTAR PUSTAKA

Alfina, & Syafrinal. (2022a). Model Sistem Verifikasi Dokumen Ijazah Digital Berbasis Teknologi Blockchain. *SMARTICS Journal*, *8*(2), 59–65. https://doi.org/10.21067/10.21067/smartics.v8i2.7718

Alfina, & Syafrinal. (2022b). Model Sistem Verifikasi Dokumen Ijazah Digital Berbasis Teknologi Blockchain. *SMARTICS Journal*, *8*(2), 59–65. https://doi.org/10.21067/10.21067/smartics.v8i2.7718

Argani, A., & Taraka, W. (n.d.). *Pemanfaatan Teknologi Blockchain Untuk Mengoptimalkan Keamanan Sertifikat Pada Perguruan Tinggi*.

Arwani, A., & Priyadi, U. (2024). Eksplorasi Peran Teknologi Blockchain dalam Meningkatkan Transparansi dan Akuntabilitas dalam Keuangan Islam: Tinjauan Sistematis. *JURNAL EKONOMI BISNIS DAN MANAJEMEN*, *2*(2), 23–37. https://doi.org/10.59024/jise.v2i2.653

Azanuddin, A., Yakub, S., & Prayudha, J. (2022). Implementasi Keamanan Citra Menggunakan Algoritma AES-128 Dengan Aplikasi Client-Server. *Jurasik (Jurnal Riset Sistem Informasi Dan Teknik Informatika)*, *7*(1), 51. https://doi.org/10.30645/jurasik.v7i1.415

Hanan, M., & Jihaannuriy, A. (2022). *Pengenalan Pelat Nomor Otomatis Menggunakan Metode Inception-ResNet v2 Skripsi Disusun Oleh*.

Ii, B. A. B. (2008). *06. Bab II_Muhammad Farhan Rochmatullah_4302190147*. 16–29.

Iqbal, T., Ahmad, L., Studi Manajemen Informatika, P., Indonesia Banda Aceh Kota, S., Banda Aceh, K., & Aceh, P. (2024). Menerapkan Blockchain untuk Meningkatkan Transparansi dan Keamanan Rantai Pasokan: Studi Kasus di Industri Kelapa Sawit. *Jurnal Manajemen Dan Teknologi (JMT)*, *1*(1). https://doi.org/10.35870/jmt.vxix.775

Joshua P Nugraha. (n.d.). *PENERAPAN BLOCKCHAIN UNTUK PENCEGAHAN SERTIPIKAT TANAH GANDA DI KEMENTERIAN AGRARIA DAN TATA RUANG BADAN PERTANAHAN NASIONAL*.

Kadly, E. I., Rosadi, S. D., & Gultom, E. (2021). Keabsahan Blockchain-Smart Contract Dalam Transaksi Elektronik: Indonesia, Amerika Dan Singapura. *Jurnal Sains Sosio Humaniora*, *5*(1), 199–212. https://doi.org/10.22437/jssh.v5i1.14128

Nainggolan, S. (2022). RESOLUSI : Rekayasa Teknik Informatika dan Informasi Implementasi Algoritma SHA-256 Pada Aplikasi Duplicate

Document Scanner. *Media Online*, *2*(5), 201–213. https://djournals.com/resolusi

Oknora Firza, S., & Ilmu Komputer, F. (2024). *Teknologi Blockchain dalam Keamanan Sertifikat Menggunakan Smart Contracts dan Distributed Ledger pada Platfrom Edutech* (Vol. 5, Issue 2).

Poetro, B. S. W., Studi, P., Informatika, T., & Diponegoro, U. (2010). Kriptografi Citra Digital dengan Algoritma Rijndael dan Transformasi Wavelet Diskrit Haar. *Prosiding Seminar Nasional Ilmu Komputer Universitas Diponegoro*, 175–178.

Pratomo, D. N., Kusumaning Putri, D. U., & Azhari, A. (2022). Implementasi Optical Character Recognition berbasis Deep Learning untuk Ekstraksi Data Sertifikat Tanah. *Jurnal Informatika: Jurnal Pengembangan IT*, *7*(3), 131–134. https://doi.org/10.30591/jpit.v7i3.3657

Rika Widianita, D. (2023). PENERAPAN ETHEREUM BLOCKCHAIN UNTUK SISTEM DATA SHARING PADA GAME SIMULASI PERAKITAN KOMPUTER BERBASIS VIRTUAL REALITY. *AT-TAWASSUTH: Jurnal Ekonomi Islam*, *VIII*(I), 1–19.

Satria, W., & Antares, J. (2022). Steganografi Metode Least Significant Bit (LSB) Dan End Of File (EoF) Pada Keamanan Data Digital. *Jurnal Teknologi Informasi*, *6*(2), 252–257.

Swasono, N. E., Himamunanto, A. R., Budiati, H., & Immanuel, U. K. (2024). *Recognition of Letter Characters in Handwritten Images Using Convolutional Neural Network and K-Means Clustering Algorithm Pengenalan Karakter Huruf pada Gambar Tulisan Tangan Menggunakan Algoritma Convolutional Neural Network dan K-Means Clustering*. *4*(October), 1646–1656.

Syahdilan, A., & Prawira, M. A. (2024). *IMPLEMENTASI ALGORITMA DISCRETE WAVELET TRANSFORM UNTUK MENAMBAHKAN INVISIBLE WATERMARKING PADA CITRA DIGITAL*. *8*(6), 12205–12217.

Syahronny, M. R., & Dewayanto, T. (2024). PENERAPAN TEKNOLOGI ARTIFICIAL INTELLIGENCE DAN BLOCKCHAIN DALAM MENDETEKSI FRAUD PADA PROSES AUDIT: SYSTEMATIC LITERATURE REVIEW. *DIPONEGORO JOURNAL OF ACCOUNTING*, *13*(3), 1–14. http://ejournal-s1.undip.ac.id/index.php/accounting

Timothy Harlian, Yudha Purwanto, & MuhammadFarisRuriawan. (2022). *Implementasi Blockchain Untuk Pendataan Dokumen Digital (Implementation of Blockchain for Digital Document Data Collection)*. *9*(3), 1076–1079.

Yogiyanti, E., & Suartana, I. M. (2024). Penerapan Teknologi Blockchain pada Sistem Laporan Keuangan Aplikasi Point of Sale. *Journal of Informatics and Computer Science*, *06*, 179–188.

Zufria, I., Ramadhan Nasution, Y., & Alfiansyah, R. (2015). Analisis Algoritma Sha-256 Pada Proses Mining Teknologi Blockchain Bitcoin. In *Angewandte Chemie International Edition, 6(11), 951–952.* (Vol. 1, Issue April).