ISSN: 2614-6754 (print)
ISSN: 2614-3097(online)

Halaman 14538-14546
Volume 9 Nomor 2 Tahun 2025

Implementasi QR Code sebagai Digital Signature Menggunakan Algoritma Advanced Encryption Standard (AES) untuk Pengamanan Surat Pada Sistem Akademik dan Kemahasiswaan

Filipo Mainzaghi[1], Hadi Kurnia Saputra[2], Dedy Irfan[3], Agariadne Dwinggo Samala[4]
[1,2,3,4] Informatika, Universitas Negeri Padang
e-mail: filipomainzaghi12@gmail.com

Abstrak

Suatu perusahaan atau organisasi menggunakan surat sebagai sarana komunikasi dengan pihak di luar maupun di dalam perusahaan atau organisasi. Surat juga menjadi sarana komunikasi terpenting dalam berbagai bidang seperti pendidikan,bisnis dan lain-lain. Salah satu cara perusahaan atau organisasi dalam memproses surat di era digital adalah dengan menerapkan sebuah sistem dokumen digital seperti penggunaan *Digital Signature* sebagai pengganti tanda tangan manual. Tanda tangan digital yang dimodifikasi secara kriptografis disimpan dalam bentuk QR Code. Untuk mempermudah dalam proses surat menyurat, maka perlu adanya pengembangan sistem dengan memanfaatkan perkembangan teknologi yaitu seperti menerapkan QR Code sebagai *Digital Signature*. Penelitian ini bertujuan untuk meningkatkan keamanan surat dengan menerapkan QR Code sebagai Digital Signature menggunakan algoritma kriptografi Advanced Encryption Standard (AES). Dengan adanya digital signature, surat akan sulit dipalsukan karena disetiap surat memiliki digital signature yang berbeda.

Kata kunci: *Surat, Digital Signature, QR Code, Kriptografi, AES*

Abstract

A company or organization uses letters as a means of communication with parties outside or inside the company or organization. Letters are also the most important means of communication in various fields such as education, business and others. One way for companies or organizations to process letters in the digital era is to implement a digital document system such as the use of Digital Signature as a substitute for manual signatures. Cryptographically modified digital signatures are stored in the form of QR Codes. To facilitate the process of correspondence, it is necessary to develop a system by utilizing technological developments, such as implementing QR Codes as Digital Signatures. This study aims to improve letter security by implementing QR Codes as Digital Signatures using the Advanced Encryption Standard (AES) cryptographic algorithm. With a digital signature, letters will be difficult to forge because each letter has a different digital signature.

Keywords : *Letter, Digital Signature, QR Code, Cryptographic, AES*

PENDAHULUAN

Suatu perusahaan atau organisasi menggunakan surat sebagai sarana komunikasi dengan pihak di luar maupun di dalam perusahaan atau organisasi. Surat juga menjadi sarana komunikasi terpenting dalam berbagai bidang seperti pendidikan,bisnis dan lain-lain. Keaslian surat ditandai dengan adanya tanda tangan yang langsung dilakukan oleh pihak pengirim secara manual. Namun Tanda tangan manual membutuhkan proses panjang mulai dari pemisahan dokumen, pendistribusian hingga sampai pada penanda tangan[1] .

Perkembangan teknologi di era digital yang semakin pesat menuntut kita untuk mengikuti arus perkembangan tersebut, begitu juga bagi perusahaan atau organisasi seperti dalam proses surat menyurat. Salah satu cara perusahaan atau organisasi dalam memproses surat di era digital adalah dengan menerapkan sebuah sistem dokumen digital seperti penggunaan *Digital Signature* sebagai pengganti tanda tangan manual.[2]

Tanda tangan *(Digital Signature)* adalah sebuah skema yang mengidentifikasikan seorang pengirim sekaligus sebagai bukti keaslian dokumen digital sehingga menjadi bukti sah dalam proses surat menyurat [3]. tangan digital adalah tanda tangan elektronik yang digunakan untuk membuktikan keaslian identitas si pengirim dari suatu pesan atau dokumen.[4]

QR Code, kependekan dari Quick Response Code, adalah gambar dua dimensi yang dapat menyimpan informasi. QRCode banyak digunakan untuk menyimpan informasi dalam bentuk teks, baik itu kode numerik, alfanumerik, atau biner. Kode QR banyak digunakan untuk tujuan komersial, biasanya berisi tautan URL ke alamat tertentu atau hanya teks biasa yang berisi iklan, promosi, dll.[5]

QR Code dapat diimplementasikan menggunakan algortima Kriptografi. Kriptografi muncul dalam konteks komunikasi jarak jauh dan pertukaran informasi, dimana komunikasi dan pertukaran informasi antar wilayah dan negara atau benua tidak lagi menjadi hambatan utama[6]. Pada saat yang sama, persyaratan keamanan untuk kerahasiaan informasi yang dipertukarkan antara meningkat. Begitu banyak pengguna, seperti Kementerian Pertahanan, perusahaan, atau bahkan individu, tidak ingin informasi yang mereka kirimkan diketahui orang lain atau pesaingnya atau negara lain. Oleh karena itu munculah cabang ilmu yang mempelajari tentang keamanan data atau dikenal sebagai kriptografi.

Advanced Encryption Standard (AES) adalah algoritma enkripsi yang dapat digunakan untuk melindungi data. Algoritma AES adalah cipher blok simetris yang dapat mengenkripsi dan mendekripsi informasi. Enkripsi mengubah data menjadi ciphertext yang tidak dapat dibaca, sebaliknya dekripsi mengubah ciphertext data menjadi bentuk aslinya, yang kita sebut plaintext. Algoritma AES ini menggunakan kunci enkripsi 128 bit, 192 bit, dan 256-bit untuk mengenkripsi dan mendekripsi data dalam potongan 128-bit.[7]

Sistem informasi merupakan salah satu hal yang sangat penting dalam sebuah perusahaan. Melalui sistem informasi, organisasi atau perusahaan dapat menjamin kualitas informasi yang diberikan dan mengambil keputusan berdasarkan informasi yang cepat, akurat dan tepat. Oleh karena itu keberadaan sistem informasi sudah menjadi kebutuhan mutlak bagi perusahaan dalam menjalankan proses bisnisnya [8]. Sistem informasi dirancang dan dibangun dengan baik untuk meningkatkan produktivitas, menghilangkan pemborosan aktivitas, meningkatkan pelayanan, mengkoordinasikan setiap bagian organisasi, dan meningkatkan kualitas kebijakan manajemen. Sistem informasi yang baik tidak hanya digunakan untuk penyimpanan data secara elektronik, tetapi juga harus mendukung proses analisis yang dibutuhkan oleh pihak manajemen, karena dengan laporan yang disajikan dengan cepat dan dapat dipanggil kapan saja, keputusan dapat dibuat lebih cepat dan lebih banyak. efisien. sesuai dengan dinamika pasar saat ini[9].

Sistem informasi AKAMA FT UNP merupakan sebuah sistem informasi yang digunakan untuk melakukan pengurusan surat khususnya surat penelitian, surat kemahasiswaan dan surat yang berkaitan dengan Praktek Lapangan Industri (PLI). Tujuan dibuat system informasi ini untuk mempersingkat waktu dan mempermudah mahasiswa dalam pengurusan surat[10]. System informasi ini dibuat hanya dikhususkan untuk pengurusan yang berkaitan dengan kegiatan akademik mahasiswa.

METODE

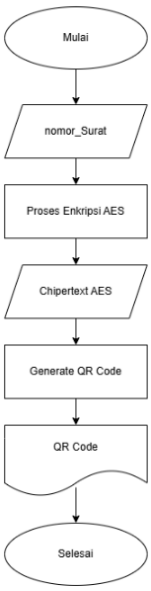
Implementasi QR Code Sebagai Digital Signature Menggunakan Algoritma Advanced Encryption Standard (AES) Untuk Pengamanan Surat Pada Sistem Akademik dan Kemahasiswaan ini menggunakan metode SDLC *Waterfall*. Metode SDLC *Waterfall* merupakan salah satu metodologi pengembangan sistem yang paling sederhana tidak berbelit-belit karena menggunakan pendekatan sistematis dan berurutan. Pada bab ini dilakukan tahapan – tahapan dalam metode *Waterfall* yang meliputi : *Analysis Requirement*, *Design*, *Implementation and Coding*, *Program Testing,* dan *Implementation and maintenance*

Analysis Requirement

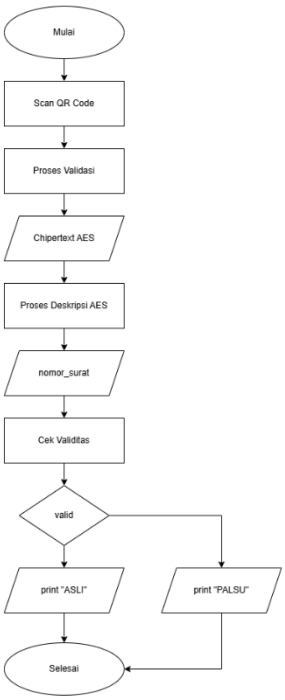
Analisysis Requirement merupakan tahap dasar dalam pengembangan sistem yang harus dilakukan setelah perancangan sistem untuk kemudian dilanjutkan dengan perancangan sistem

ISSN: 2614-6754 (print)
ISSN: 2614-3097(online)

Halaman 14538-14546
Volume 9 Nomor 2 Tahun 2025



Gambar 1. Flowchart Proses Enkripsi



Gambar 2. Flowchart Proses Dekripsi

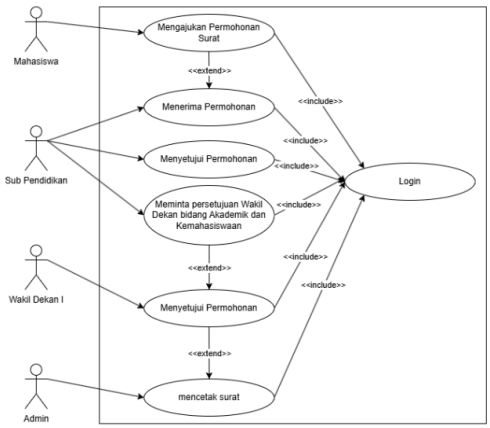
Proses enkripsi dimulai dari mengambil nomor surat kemudian dienkripsi menggunakan algoritma Advanced Encryption Standard (AES) dan chipertext dari hasil enkripsi digenerate menjadi QR Code. Proses dekripsi dimulai dengan menscan QR Code kemudian data yang ada pada QR Code di dekripsi, plain text hasil dekripsi akan dicocokan dengan data yang ada pada database

Design System

Design System adalah langkah untuk menyusun rancangan berdasarkan hasil analisis sebelumnya, tujuannya agar sistem yang dibuat nantinya sesuai dan berfungsi dengan baik.

Use Case Diagram

Use Case Diagram adalah Langkah yang digunakan untuk menggambarkan hubungan antara pengguna dan fungsi-fungsi sistem yang ada dalam suatu sistem. Tujuan utama dari analisis sistem yang berguna untuk memperjelas langkah kerja dan konsep perancangan dengan unsur-unsur yang terlibat dalam sistem.



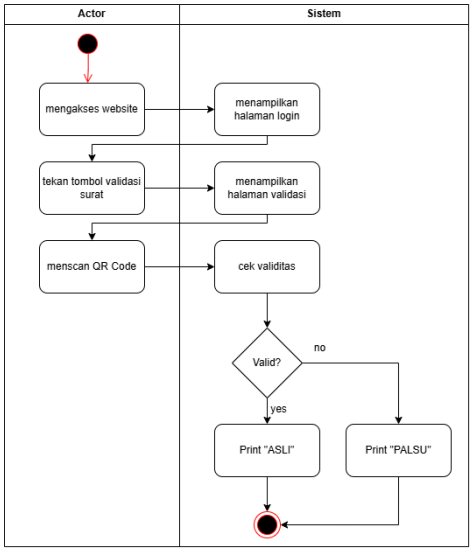
Gambar 3. Use Case Diagram

ISSN: 2614-6754 (print)
ISSN: 2614-3097(online)
Halaman 14538-14546
Volume 9 Nomor 2 Tahun 2025

Activity Diagram

Activity Diagram adalah salah satu diagram dalam *Unified Modeling Language* (UML) yang digunakan untuk memodelkan alur kerja atau aktivitas dalam suatu sistem. Diagram ini menggambarkan langkah-langkah proses yang dilakukan oleh sistem, mulai dari awal hingga selesai, termasuk pengambilan keputusan, proses paralel, atau transisi antar aktivitas.

Activity Diagram Validasi Surat

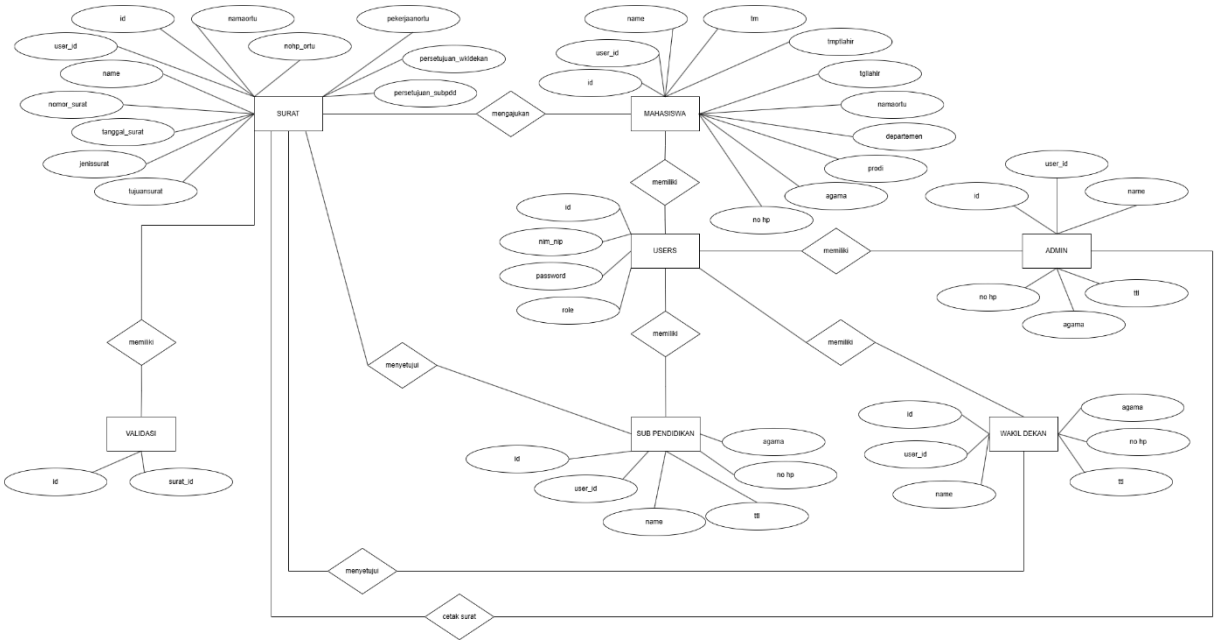


Gambar 4. Activity Diagram Validasi Surat

Actor mengakses halaman validasi surat pada sistem informasi akademik dan kemahasiswaan. Kemudian menscan QR Code pada surat, jika data tidak ditemukan maka akan muncul peringatan surat palsu,dan jika data ada maka akan muncul keterangan surat asli dan muncul informasi yang tersimpan dalam QR Code tersebut

Entity Relationship Diagram

ERD merupakan diagram yang menggambarkan hubungan antar entitas, atribut, dan relasi dalam sebuah sistem, terutama dalam perancangan basis data.

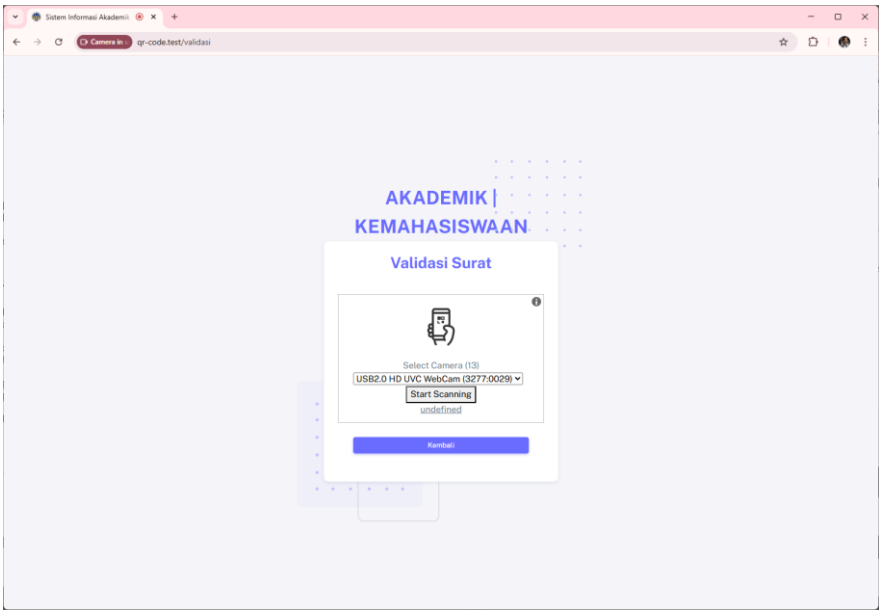


Gambar 5. Entity Relationship Diagram

HASIL DAN PEMBAHASAN

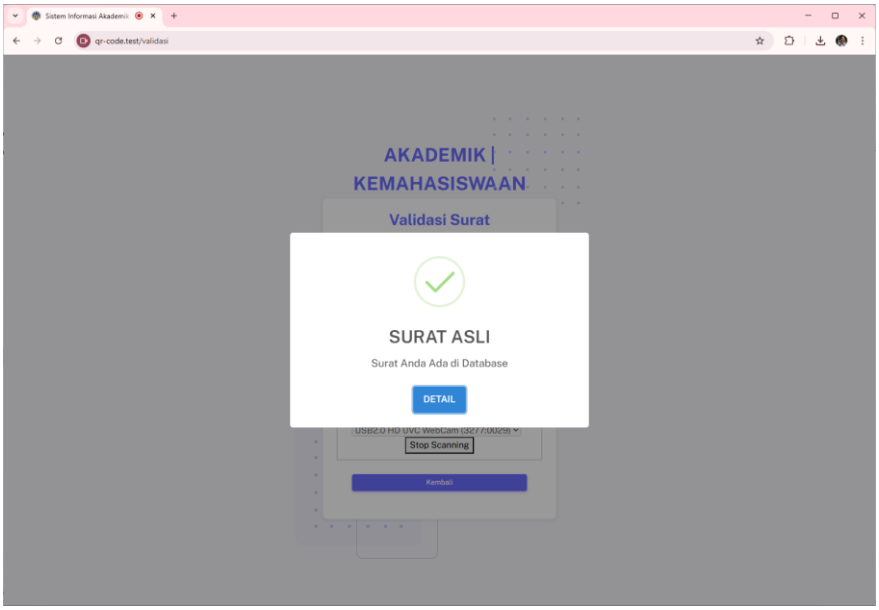
Halaman validasi

Halaman validasi adalah halaman dimana actor melakukan pengecekan surat menggunakan QR Code Scanner.



Gambar 6. Halaman Validasi

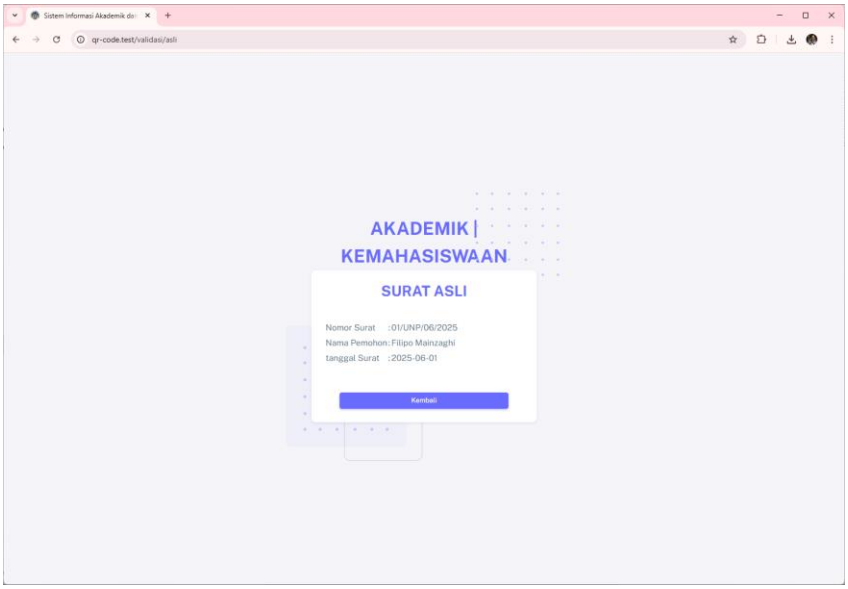
Halaman Surat Asli



Gambar 7. Tampilan Surat Asli

ISSN: 2614-6754 (print)
ISSN: 2614-3097(online)

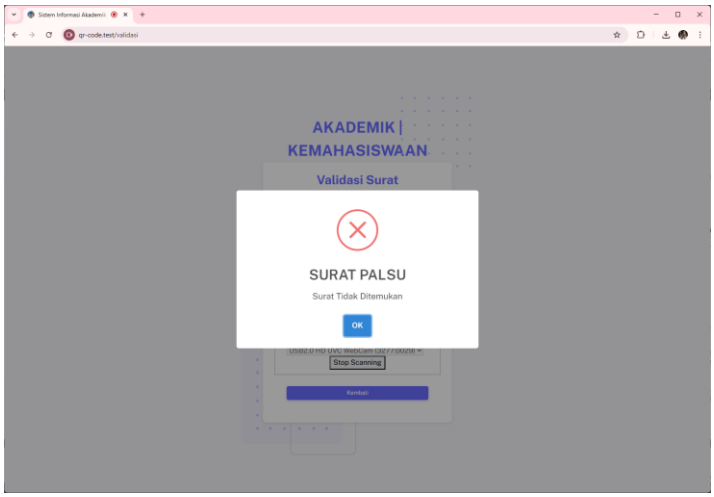
Halaman 14538-14546
Volume 9 Nomor 2 Tahun 2025



Gambar 8. Tampilan Data Surat yang tersimpan di QR Code

Halaman ini ditampilkan apabila data yang terdapat pada QR Code ada pada database.

Halaman Surat Palsu



Gambar 9. Tampilan Halaman Surat palsu

Halaman ini ditampilkan apabila data yang terdapat pada QR Code tidak ada pada database.

Testing

Testing bertujuan untuk menemukan kesalahan dalam sistem yang sedang dibangun. Pada tahap ini, akan dilakukan pengujian terhadap pengamanan surat yang menggunakan QR Code sebagai digital signature. Pengujian akan dilakukan menggunakan metode blackbox. Tahap pengujian ini bertujuan untuk memastikan data yang tersimpan pada QR Code sama dengan data yang ada di surat.

Pengujian menggunakan QR Code Asli

KEMENTERIAN RISET, TEKNOLOGI DAN PENDIDIKAN TINGGI
UNIVERSITAS NEGERI PADANG
FAKULTAS TEKNIK
Jl.Prof Dr. Hamka Kampus UNP Air Tawar Padang 25131
Telp (0751) 7055644 e-mail: info@ft.unp..ac.id

SURAT KETERANGAN AKTIF KULIAH
01/UNP/06/2025

Dekan Fakultas Teknik Universitas Negeri Padang, dengan ini menyatakan bahwa :

Nama	:	Filipo Mainzaghi
Tempat / Tanggal Lahir	:	Padang/2000-05-08
TM / NIM	:	2018 / 18076004
Departemen / Prodi	:	Teknik Elektronika / Pendidikan Teknik Informatika dan Komputer

Yang bersangkutan adalah mahasiswa Departemen Teknik Elektronika Fakultas Teknik Universitas Negeri Padang dan anak dari :

Nama	:	HELMI
Pekerjaan	:	Buruh Harian Lepas
Alamat	:	Tabing Banda Gadang RT.005/RW.001

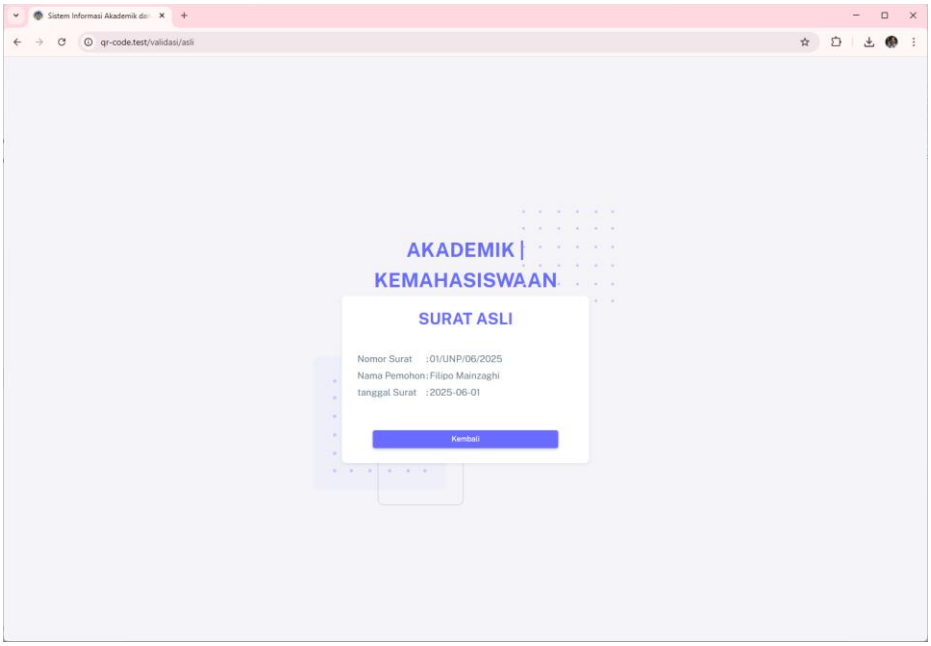
Demikian Surat keterangan ini dibuat untuk dapat dipergunakan sebagaimana mestinya.

Padang, Mei 2025
An. Dekan
Wakil Dekan I

Dr. Fadhilah, S.Pd, M.Si
NIP:195209111981031003

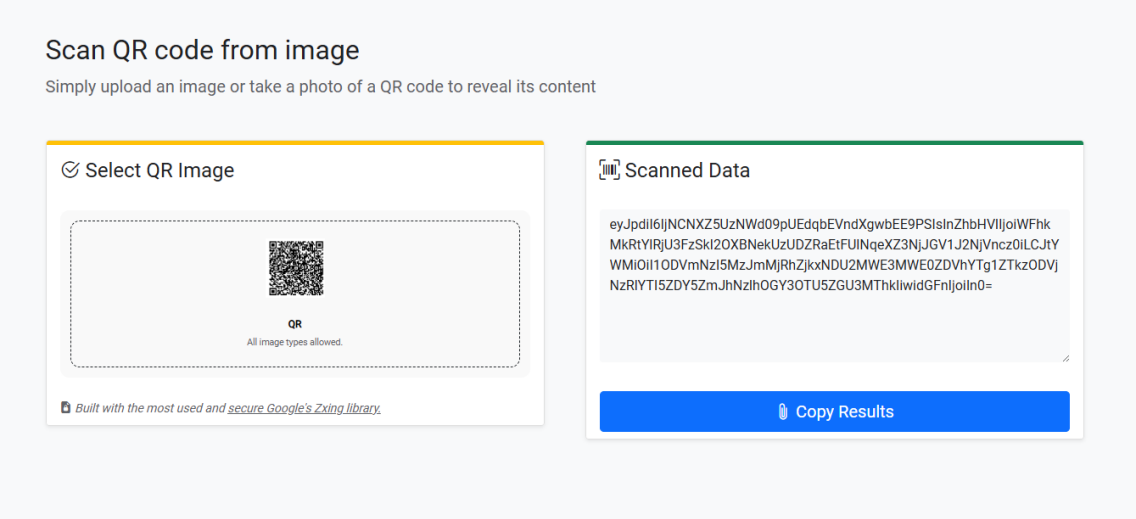
Gambar 10. Surat Asli

Apabila seseorang mencoba menscan QR Code pada surat diatas pada halaman validasi surat maka akan muncul data seperti berikut :



Gambar 11. Data pada surat asli

Apabila seseorang mencoba menscan QR Code pada surat menggunakan aplikasi scanner lain maka akan muncul data seperti berikut :

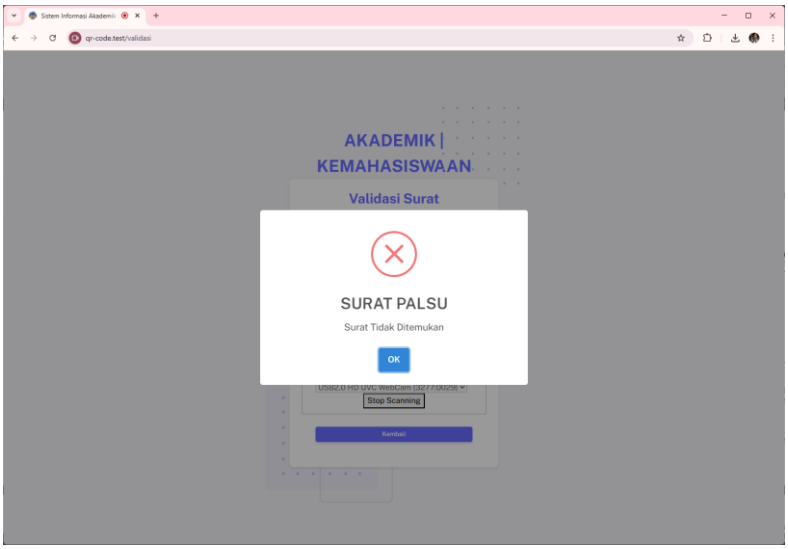


Gambar 12. Hasil Scan menggunakan Scanner lain

Pengujian menggunakan QR Code Palsu

Gambar 13. QR Code Palsu

Apabila seseorang mencoba menscan QR Code Palsu maka akan muncul data seperti berikut :



Gambar 14. Tampilan Surat palsu

SIMPULAN

Setelah dilakukan pengujian terhadap keamanan surat dengan menscan QR Code pada surat, dapat disimpulkan bahwa sistem dapat mendeteksi surat asli atau palsu dengan mencocokan data yang tersimpan pada QR Code dengan data yang tersimpan pada database. Apabila seseorang mencoba menscan QR Code menggunakan aplikasi scanner lain maka yang muncul hanya chipertext dari QR Code tersebut, dimana harus mempunyai kunci untuk mendekripsi chipertext tersebut.

DAFTAR PUSTAKA

Putri Pratiwi, Binar., Riyan Pratama, Mudafiq. (2019). Implementasi Algoritma AES (Advanced Encryption Standard) dan RSA (Rivest Shamir Adleman) untuk Pengamanan Surat di Humanika. *Seminar Nasional Teknik Elektro Dan Informatika*, *2*(2), 1003–1043.

Andi Kriswanto, E., Studi Teknik Informatika, P., Banjarbaru, S., Yani Km, J. A., & Selatan, K. (n.d.). *Implementasi Digital Signature Untuk Validasi Disposisi Surat*.

Ferzha Putra Utama., Murfid Aqil., Hanan Raihana., (2022). *Implementasi Tanda Tangan Digital pada Surat Keterangan Bebas Laboratorium*

Nuraeni, F., Handoko Agustin, Y., Kurniadi, D., Dewi Ariyanti, I., Tinggi Teknologi Garut Jl Mayor Syamsu No, S., Tarogong Kidul, K., & Garut, K. (2020). *Implementasi Skema QR-Code dan Digital Signature menggunakan Kombinasi Algoritma RSA dan AES untuk Pengamanan Data Sertifikat Elektronik* (Issue SNTIKI).

Pasca Nugraha, M., Rinaldi Munir, I. M. (n.d.). *Pengembangan Aplikasi QR Code Generator dan QR Code Reader dari Data Berbentuk Image*.

M. Miftakul Amin., (2016). *Implementasi kriptografi klasik pada Komunikasi berbasis teks*

Taufan Abdurrachman., Bernard Renaldy S.., (2021). *Pengembangan Sistem Informasi Asosiasi Jasa Konstruksi dengan Menerapkan Tanda Tangan Digital.*

Yaya Suharya, S.Kom.,M.T, Hani Widia., (2020).*Implementasi Digital Signature Menggunakan Algoritma Kriftografi Rsa Untuk Pengamanan Data Di Smk Wirakarya 1 Ciparay*

Anita Oktaviyana., Maria Mercedes B., (2024). *Analisis Sistem Informasi Manajemen*

Salsabila Kameliya Putri1., Thamrin., (2023). *Pengembangan Sistem Informasi Monitoring Pengalaman Lapangan Industri (PLI) Di Departemen Teknik Elektronika Universitas Negeri Padang*