Masuk: 21 Agustus 2025 | Revisi: 17 September 2025 | Diterima: 26 Oktober 2025
e-SSIN: 3031-3082; DOI: https://doi.org/10.26618/k6zs6353

jumptech

Implementasi Tanda Tangan Digital dengan Metode AES dan Deflate untuk Verifikasi Surat Permohonan KKP

Muhammad Ikhsan Nur[1] | Lukman[*2] | Muhyiddin A M Hayat[2]

1 Mahasiswa Program Studi Informatika, Fakultas Teknik, Universitas Muhammadiyah Makassar, Indonesia.
Email: 105841100820@unismuh.ac.id

2 Program Studi Informatika, Fakultas Teknik, Universitas Muhammadiyah Makassar, Indonesia.
Email: lukman@unismuh.ac.id; muhyiddin@unismuh.ac.id;

Korespondensi:
*Lukman
lukman@unismuh.ac.id

ABSTRAK
Transformasi digital di lingkungan akademik menuntut adanya sistem verifikasi dokumen yang aman, efisien, dan mudah diimplementasikan. Penelitian ini bertujuan untuk mengimplementasikan tanda tangan digital dalam proses verifikasi Surat Permohonan Kuliah Kerja Profesi (KKP) dengan mengombinasikan algoritma *Advanced Encryption Standard (AES)* dan metode kompresi *Deflate*. Sistem dirancang melalui beberapa tahapan, meliputi *preprocessing* data surat untuk menggabungkan seluruh informasi penting ke dalam satu format string, kompresi data menggunakan metode *Deflate*, serta enkripsi menggunakan algoritma AES-128 dengan mode *Cipher Block Chaining (CBC)*. Data terenkripsi selanjutnya dikonversi ke dalam bentuk *QR Code* yang berfungsi sebagai representasi tanda tangan digital. Proses verifikasi dilakukan dengan memindai *QR Code* menggunakan aplikasi *client*, kemudian dilakukan tahap dekripsi dan dekompresi untuk mengembalikan data ke bentuk aslinya. Hasil pengujian menunjukkan bahwa sistem mampu menjaga kerahasiaan dan integritas data, mempercepat proses verifikasi administrasi, serta meminimalkan potensi kesalahan manusia dalam pengelolaan dokumen. Dengan demikian, integrasi algoritma AES dan metode *Deflate* dapat diterapkan secara efektif sebagai solusi verifikasi dokumen digital di lingkungan akademik.

Kata Kunci: Tanda Tangan Digital, AES, *Deflate*, Enkripsi, Dokumen Akademik

ABSTRACT
Digital transformation in academic environments requires a document verification system that is secure, efficient, and easy to implement. This study aims to implement a digital signature system for verifying Internship Application Letters (Kuliah Kerja Profesi/KKP) by combining the Advanced Encryption Standard (AES) algorithm and the Deflate compression method. The system is designed through several stages, including preprocessing of letter data to merge essential information into a single string format, data compression using the Deflate method, and encryption using the AES-128 algorithm in Cipher Block Chaining (CBC) mode. The encrypted data is then converted into a QR Code, which serves as a digital signature representation. The verification process is carried out by scanning the QR Code using a client application, followed by decryption and decompression to restore the original data. The testing results indicate that the proposed system is capable of maintaining data confidentiality and integrity, accelerating administrative verification processes, and reducing human error in document management. Therefore, the integration of AES and Deflate proves to be an effective solution for digital document verification in academic institutions.

Keyworsds: *Digital Signature, AES, Deflate, Encryption, Academic Document*

1 | PENDAHULUAN

Dalam proses pembuatan Surat Permohonan Kuliah Kerja Profesi (KKP) di Fakultas Teknik Universitas Muhammadiyah (UNISMUH) Makassar, staf administrasi sering menghadapi tantangan dalam memverifikasi keaslian surat. Proses verifikasi yang masih dilakukan secara manual, yaitu dengan memeriksa data secara daring melalui komputer, menyebabkan keterlambatan pelayanan serta meningkatkan potensi terjadinya kesalahan manusia. Kondisi ini menunjukkan perlunya sistem verifikasi yang lebih efisien dan andal. Penerapan tanda tangan digital menjadi salah satu solusi yang mampu meningkatkan efisiensi, akurasi, dan kecepatan proses verifikasi dokumen akademik serta telah terbukti efektif dalam mendukung sistem administrasi akademik di perguruan tinggi (Fatma et al., 2023; Purnama et al., 2021).

Tanda tangan digital merupakan skema matematis yang memungkinkan validasi keaslian suatu dokumen elektronik tanpa memerlukan pemeriksaan manual. Keunggulan utama tanda tangan digital terletak pada kemampuannya dalam menjamin integritas, autentikasi, dan non-repudiation dokumen, sehingga dokumen terlindungi dari perubahan maupun pemalsuan yang tidak sah (Sharma & Gupta, 2021; Pemayun & Dewi, 2025). Dalam implementasinya, tanda tangan digital bekerja dengan mekanisme kriptografi asimetris yang memanfaatkan pasangan kunci *privat* dan kunci publik untuk memastikan bahwa hanya pihak yang berwenang yang dapat menandatangani dan memverifikasi dokumen elektronik (Alsaedi & Burnap, 2020; El Makkaoui et al., 2021).

Selain menjamin keaslian dokumen, sistem tanda tangan digital juga berperan penting dalam meningkatkan keamanan alur kerja (*workflow*) verifikasi dokumen. Integrasi tanda tangan digital dalam sistem administrasi terbukti mampu mempercepat proses validasi, mengurangi ketergantungan pada verifikasi manual, serta meningkatkan kepercayaan terhadap dokumen elektronik yang digunakan dalam lingkungan institusi formal (Hussain & Shah, 2022).

Dalam konteks keamanan dokumen elektronik, algoritma *Advanced Encryption Standard (AES)* menjadi pilihan yang efektif untuk melindungi informasi dari akses tidak sah. AES merupakan algoritma enkripsi simetris yang mendukung ukuran kunci 128, 192, dan 256 bit, sehingga memberikan tingkat keamanan yang tinggi dan stabil untuk berbagai kebutuhan sistem informasi, termasuk aplikasi berbasis *mobile*. Beberapa penelitian menunjukkan bahwa implementasi AES yang dioptimalkan untuk lingkungan *mobile* mampu menjaga keseimbangan antara keamanan dan efisiensi komputasi, sehingga sesuai digunakan pada sistem verifikasi dokumen digital yang membutuhkan kecepatan pemrosesan tinggi (Fahlevvi et al., 2025; Li et al., 2022). Selain itu, teknik kompresi *Deflate* dapat diterapkan sebelum proses enkripsi untuk mengurangi ukuran data, sehingga mempercepat proses enkripsi dan dekripsi tanpa mengurangi keutuhan maupun keabsahan informasi (Sujono et al., 2020).

Untuk mendukung proses verifikasi dokumen secara praktis, data hasil enkripsi dapat direpresentasikan dalam bentuk *Quick Response (QR) Code*. *QR Code* memungkinkan proses autentikasi dokumen dilakukan secara cepat, baik pada dokumen digital maupun cetak, selama dikombinasikan dengan mekanisme kriptografi yang tepat. Namun demikian, *QR Code* juga memiliki potensi kerentanan apabila tidak dilindungi dengan sistem keamanan yang memadai, sehingga perlu diintegrasikan dengan algoritma enkripsi yang kuat (Rahman & Hossain, 2020; Kumar & Tripathi, 2020).

Dengan mengintegrasikan tanda tangan digital berbasis AES dan metode kompresi *Deflate*, proses verifikasi keaslian surat dapat dilakukan secara *offline* tanpa memerlukan akses langsung ke komputer administrasi. Pendekatan ini tidak hanya mempercepat pelayanan dan mengurangi risiko kesalahan manusia, tetapi juga meningkatkan keamanan serta keabsahan dokumen secara hukum. Implementasi sistem verifikasi dokumen digital yang terstruktur dan aman sangat penting untuk mendukung transformasi digital di lingkungan akademik dan meningkatkan efisiensi operasional institusi pendidikan tinggi (Kustiyandi et al., 2021; Indriani et al., 2024).

2 | METODE

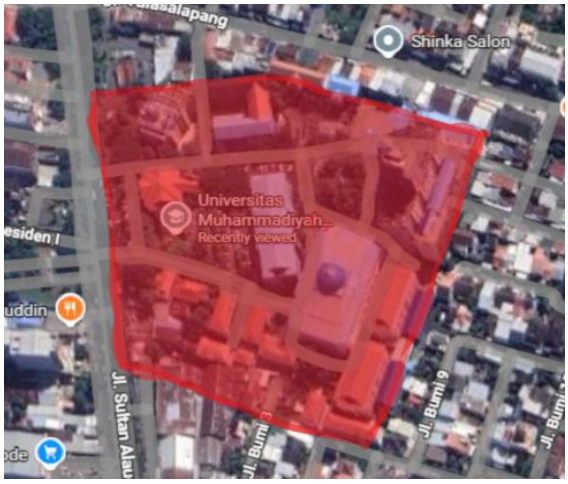
Metodologi Metodologi penelitian ini dirancang untuk mendukung implementasi sistem tanda tangan digital pada proses verifikasi Surat Permohonan Kuliah Kerja Profesi (KKP) dengan menitikberatkan pada aspek keamanan, efisiensi, dan keandalan data. Pendekatan penelitian yang digunakan bersifat implementatif dan analitis dengan mengintegrasikan metode kompresi Deflate dan algoritma enkripsi *Advanced Encryption Standard (AES)* sebagai mekanisme utama pengamanan dokumen. Kombinasi antara teknik kompresi dan enkripsi terbukti mampu meningkatkan efisiensi penyimpanan data sekaligus memperkuat perlindungan terhadap akses tidak sah serta upaya pemalsuan dokumen (Kaur & Singh, 2021; Hameed et al., 2021).

Pemilihan algoritma AES-128 dengan mode *Cipher Block Chaining (CBC)* didasarkan pada pertimbangan tingkat keamanan yang tinggi serta performa yang efisien, khususnya pada aplikasi berbasis *mobile* yang membutuhkan kecepatan pemrosesan tanpa mengorbankan kerahasiaan dan integritas data (Fadhil & Hassan, 2022; Li et al., 2022; Sari & Prasetyo, 2022), di mana efisiensi enkripsi menjadi faktor penting dalam sistem verifikasi dokumen berbasis perangkat bergerak. Selain itu, penerapan mekanisme kriptografi dalam sistem tanda tangan digital ini diselaraskan dengan prinsip dan rekomendasi keamanan yang ditetapkan dalam *Digital Signature Standard (DSS)* FIPS PUB 186-5 sebagai standar kriptografi yang diakui secara internasional (NIST, 2023).

Rangkaian proses dalam penelitian ini dimulai dari tahap pengolahan dan penyeragaman data surat untuk memastikan konsistensi format data, dilanjutkan dengan proses kompresi menggunakan metode *Deflate* guna mengoptimalkan ukuran data sebelum dienkripsi. Data hasil kompresi kemudian dienkripsi menggunakan AES-128-CBC untuk menjaga kerahasiaan dan integritas informasi selama proses penyimpanan dan distribusi. Seluruh data terenkripsi selanjutnya direpresentasikan dalam bentuk *QR Code* sebagai media verifikasi digital, sehingga proses validasi dokumen dapat dilakukan secara cepat, praktis, dan andal baik pada dokumen digital maupun cetak (Arief et al., 2021; Dey et al., 2021).

2.1 | Lokasi

Penelitian ini dilakukan di Universitas Muhammadiyah Makassar, khususnya Fakultas Teknik, yang terletak di Jl. Sultan Alauddin No.259, Kota Makassar, Sulawesi Selatan, lihat **Gambar 1**.



GAMBAR 1 Lokasi Penelitian

2.2 | Alat dan Bahan

Alat dan bahan yang digunakan dalam penelitian ini terdiri dari perangkat keras dan perangkat lunak yang mendukung proses pengembangan serta pengujian sistem tanda tangan digital.

Alat (Perangkat Keras):

- Laptop dengan sistem operasi Windows 11.
- *Smartphone* berbasis Android 10 sebagai media pemindaian *QR Code* dan proses verifikasi dokumen.

Praktik Bahan (Perangkat Lunak dan Data):

- Node.js sebagai platform pengembangan sisi server.
- React Native sebagai framework pengembangan aplikasi *client*.
- *Library* crypto (Node.js) dan crypto-js untuk proses enkripsi dan dekripsi AES-128-CBC.
- *Library* pako untuk proses kompresi *Deflate* dan dekompresi Inflate.
- *Library* qrcode untuk konversi data terenkripsi ke dalam bentuk *QR Code*.
- Data Surat Permohonan Kuliah Kerja Profesi (KKP) dalam bentuk JSON sebagai objek penelitian.

Penelitian ini merupakan penelitian implementatif yang berfokus pada pengembangan dan pengujian sistem tanda tangan digital untuk verifikasi Surat Permohonan Kuliah Kerja Profesi (KKP). Sistem diimplementasikan sebagai studi kasus pada lingkungan administrasi Fakultas Teknik Universitas Muhammadiyah Makassar.

Data penelitian berupa data Surat Permohonan KKP yang diperoleh dari bagian administrasi, meliputi identitas mahasiswa, program studi, tujuan KKP, dan informasi penandatangan surat. Data tersebut digunakan sebagai input utama dalam proses kompresi, enkripsi, dan verifikasi dokumen.

Penelitian ini menggunakan metode perancangan dan implementasi sistem tanda tangan digital berbasis AES dan *Deflate*. Data Surat Permohonan KKP diproses melalui tahapan *preprocessing*, kompresi, enkripsi, dan konversi ke *QR Code*. Tahap *preprocessing* berperan sebagai tahap awal untuk memastikan data berada dalam kondisi terstandar sebelum diproses lebih lanjut (Bansod & Patil, 2020; Dey et al., 2021).

2.3 | Pengumpulan dan Analisis Data

Pengumpulan data dilakukan dengan menghimpun dokumen Surat Permohonan Kuliah Kerja Profesi (KKP) dari Fakultas Teknik Universitas Muhammadiyah Makassar. Data yang digunakan meliputi identitas mahasiswa, NIM, program studi, serta informasi instansi tujuan pelaksanaan KKP. Proses pengambilan data dilakukan secara langsung melalui bagian administrasi untuk memastikan keakuratan dan keabsahan dokumen. Analisis data dilakukan secara deskriptif dan komparatif untuk mengevaluasi kinerja dan aspek keamanan sistem yang dikembangkan. Pengujian fungsionalitas sistem dilakukan menggunakan metode *black-box*. **Gambar 2** menunjukkan data mentah dalam bentuk *JavaScript Object Notation (JSON)* yang akan dijadikan sampel untuk penelitian ini.

```
{
 "kepada": "Bapak/Ibu Pimpinan Pt. Ide Kreatif Asia",
 "tempat_tujuan": "Pt. Ide Kreatif Asia",
 "nama_prodi": "Informatika",
 "nama_ttd": "Bapak Rektor",
 "tanggal_hijriyah": "25 Safar 1447 H",
 "tanggal_masehi": "19 Agustus 2025 M",
 "tableData": [
   {
     "no": 1,
     "nama_mahasiswa": "Muhammad Ikhsan Nur",
     "nim": "105841100820"
   },
   {
     "no": 2,
     "nama_mahasiswa": "Lis Indriani",
     "nim": "105841108020"
   },
   {
     "no": 3,
     "nama_mahasiswa": "Rizka Adrianingsih",
     "nim": "105841108520"
   }
 ]
}
```


GAMBAR 2 Data Penelitian

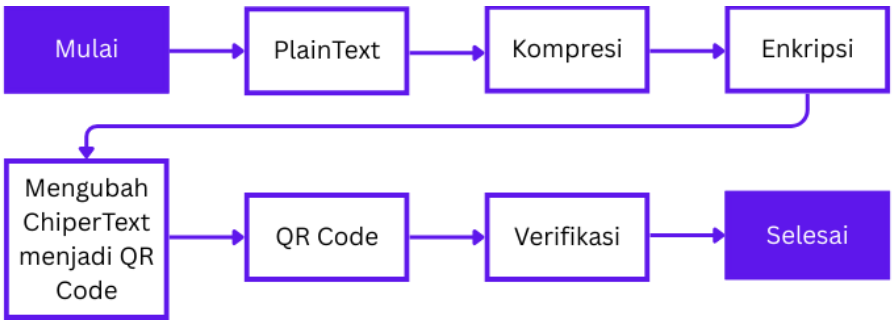
2.4 | Alur Sistem

Sistem tanda tangan digital yang diusulkan terdiri dari dua proses utama, yaitu proses pembangkitan tanda tangan digital dan proses verifikasi dokumen. Pada proses pembangkitan, data Surat Permohonan KKP terlebih dahulu melalui tahap *preprocessing* . Tahap *preprocessing* meliputi normalisasi format data, penghapusan karakter yang tidak diperlukan, serta penyusunan struktur data dalam format teks terstandar untuk memastikan konsistensi data.

Data hasil *preprocessing* selanjutnya diproses melalui tahap kompresi menggunakan metode *Deflate* dan dienkripsi menggunakan algoritma AES-128-CBC. Data terenkripsi kemudian dikonversi ke dalam bentuk *QR Code* yang ditempatkan pada dokumen surat sebagai representasi tanda tangan digital.

Pada proses verifikasi, *QR Code* dipindai menggunakan aplikasi *client* untuk memperoleh data terenkripsi. Data tersebut selanjutnya didekripsi menggunakan algoritma AES-128-CBC dan didekompresi menggunakan metode *Deflate* sehingga diperoleh kembali data surat dalam bentuk asli untuk dilakukan validasi keaslian dan integritas dokumen.

Gambar 3 menunjukkan alur sistem tanda tangan digital yang dimulai dengan pengolahan data surat Permohonan Kuliah Kerja Profesi (KKP) dalam bentuk *plaintext*. Data tersebut kemudian dikompresi menggunakan algoritma *Deflate* dengan tujuan mengurangi ukuran data sebelum dilakukan proses enkripsi. Setelah tahap kompresi, data dienkripsi menggunakan algoritma AES-128 dengan mode *Cipher Block Chaining (CBC)* sehingga dihasilkan *Ciphertext* dalam bentuk teks acak yang tidak dapat dibaca secara langsung. *Ciphertext* hasil enkripsi selanjutnya dikonversi ke dalam bentuk *QR Code* menggunakan library qrcode. *QR Code* yang dihasilkan menjadi representasi tanda tangan digital yang disematkan pada dokumen surat dan dapat dipindai kembali pada tahap verifikasi untuk proses dekripsi dan dekompresi. Dengan demikian, seluruh proses kompresi dan enkripsi dinyatakan selesai.



GAMBAR 3 Flowchart Alur Sistem Tanda Tangan Digital

2.5 | *Preprocessing* Data

Tahap *preprocessing* dilakukan sebelum proses kompresi dan enkripsi dengan tujuan menyatukan seluruh *field* data Surat Permohonan KKP ke dalam satu format string terstandar. Data yang diproses meliputi identitas penerima surat, tujuan KKP, program studi, penandatangan surat, tanggal hijriah, tanggal masehi, serta daftar mahasiswa yang mengikuti kegiatan KKP.

Gambar 4 menunjukkan hasil *preprocessing* data Surat Permohonan KKP, di mana seluruh *field* penting yang semula tersimpan dalam struktur data terpisah digabungkan ke dalam satu format string terstruktur. Data yang diproses meliputi nama penerima surat, tujuan surat, program studi, nama penandatangan, tanggal hijriah, tanggal masehi, serta daftar mahasiswa beserta NIM. Proses penggabungan ini dilakukan untuk menyederhanakan struktur data sehingga lebih efisien dalam proses kompresi dan enkripsi. Pemisahan antaratribut menggunakan karakter khusus bertujuan untuk menjaga keterbacaan sistem dan mempermudah proses rekonstruksi data pada tahap dekripsi dan dekompresi.

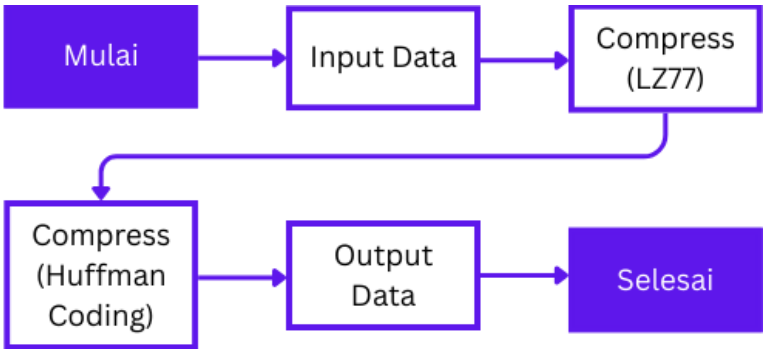
```
Bapak/Ibu Pimpinan Pt. Ide Kreatif Asia#Pt. Ide Kreatif Asia#Informatika#Bapak Rektor#25 Safar 1447 H#19 Agustus 2
025 M#1:Muhammad Ikhsan Nur:105841100820|2:Lis Indriani:105841108020|3:Rizka Adrianingsih:105841108520
```

GAMBAR 4 *Output* Data Setelah *Preprocessing*

2.6 | Kompresi Data *Deflate*

Metode *Deflate* menggabungkan algoritma LZ77 dan Huffman *Coding* untuk mengurangi ukuran data tanpa kehilangan informasi. Algoritma LZ77 berfungsi mendeteksi dan menggantikan pola data yang berulang dengan referensi tertentu, sedangkan Huffman *Coding* melakukan pengkodean berdasarkan frekuensi kemunculan data sehingga ukuran representasi biner menjadi lebih efisien. Kombinasi kedua algoritma ini memungkinkan proses kompresi data berlangsung secara optimal sebelum tahap enkripsi dilakukan (Goyal & Purohit, 2020).

Gambar 5 menunjukkan flowchart proses kompresi data menggunakan metode *Deflate*. Proses dimulai dengan data masukan berupa teks asli yang akan dikompresi. Tahap pertama menggunakan algoritma LZ77 untuk mendeteksi pola atau urutan karakter yang berulang dalam data. Ketika ditemukan pola yang sama, algoritma ini menggantinya dengan referensi berupa pasangan nilai *offset* dan *length* yang merepresentasikan posisi serta panjang urutan karakter tersebut. Hasil dari tahap LZ77 selanjutnya diproses menggunakan Huffman *Coding* untuk melakukan kompresi lanjutan. Pada tahap ini, karakter dan referensi hasil LZ77 dikodekan berdasarkan frekuensi kemunculannya, di mana karakter yang sering muncul diberikan representasi biner yang lebih pendek dibandingkan karakter yang jarang muncul. Melalui kombinasi kedua algoritma tersebut, ukuran data dapat dikurangi secara signifikan. *Output* dari proses ini berupa data terkompresi dengan ukuran yang lebih kecil dan siap digunakan pada tahap enkripsi selanjutnya.



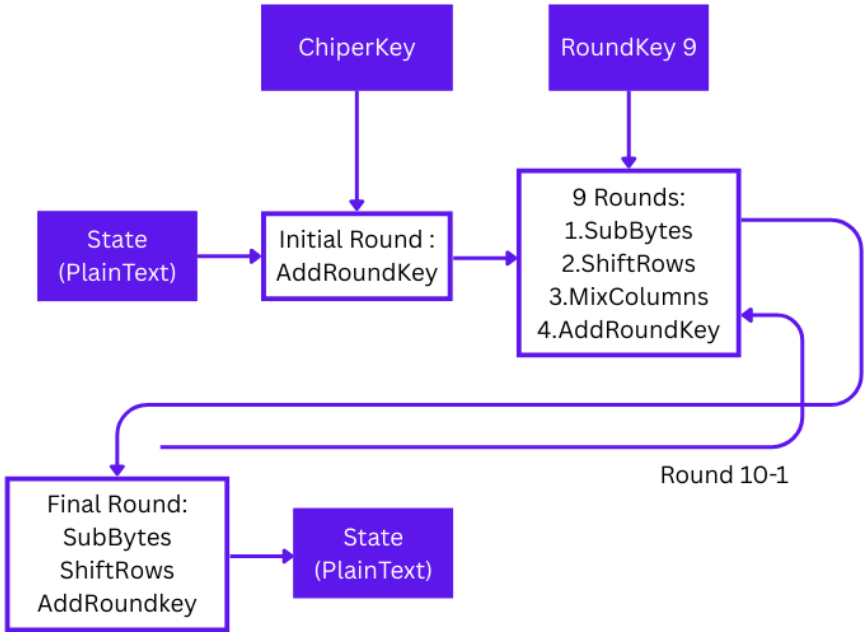
GAMBAR 5 Flowchart Proses Kompresi *Deflate*

2.7 | Enkripsi AES-128-CBC

AES-128 dengan mode *Cipher Block Chaining (CBC)* digunakan untuk mengenkripsi data hasil kompresi dengan memanfaatkan kunci simetris dan *Initialization Vector (IV)*. Penggunaan IV bertujuan untuk memastikan bahwa *Ciphertext* yang dihasilkan bersifat unik meskipun *plaintext* yang dienkripsi memiliki nilai yang sama, sehingga meningkatkan tingkat keamanan data selama proses penyimpanan dan transmisi.

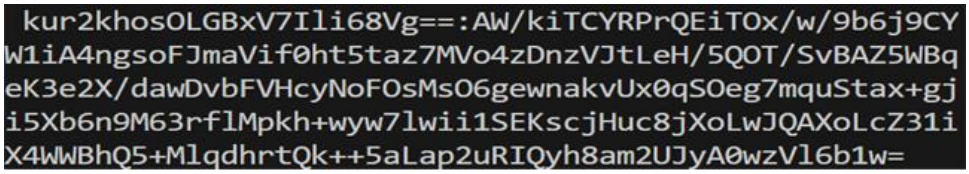
Gambar 6 memperlihatkan flowchart proses enkripsi menggunakan algoritma *Advanced Encryption Standard (AES)*. Proses enkripsi diawali dengan data masukan berupa *plaintext* yang direpresentasikan sebagai state. Pada tahap awal, dilakukan proses AddRoundKey dengan melakukan operasi XOR antara *plaintext* dan kunci enkripsi. Selanjutnya, data diproses melalui sejumlah putaran enkripsi sebanyak Nr–1 kali. Setiap putaran terdiri atas beberapa tahapan, yaitu SubBytes untuk melakukan substitusi byte menggunakan tabel S-box, ShiftRows untuk menggeser baris-baris pada state, MixColumns untuk melakukan

transformasi pada kolom state, serta AddRoundKey untuk mengombinasikan state dengan kunci putaran. Setelah seluruh putaran utama selesai, dilakukan final round yang meliputi tahapan SubBytes, ShiftRows, dan AddRoundKey tanpa proses MixColumns. Hasil akhir dari seluruh rangkaian proses enkripsi ini adalah *Ciphertext* berupa data terenkripsi yang tidak dapat dibaca secara langsung.



GAMBAR 6 Flowchart Proses Enkripsi AES

Gambar 7 menampilkan hasil enkripsi data Surat Permohonan KKP yang telah melalui tahap *preprocessing* dan kompresi *Deflate*. Data dienkripsi menggunakan algoritma AES-128-CBC sehingga menghasilkan *Ciphertext* berupa rangkaian karakter acak dalam format Base64. Bentuk data ini menunjukkan bahwa informasi asli telah berhasil diamankan dan tidak dapat dipahami secara langsung tanpa kunci dan Initialization Vector yang sesuai. Hasil enkripsi ini menjadi bukti bahwa sistem mampu menjaga kerahasiaan data sebelum disimpan atau dikonversi ke media lain untuk keperluan verifikasi.



GAMBAR 7 Hasil Enkripsi

3 | HASIL DAN PEMBAHASAN

Hasil utama dari penelitian ini ditunjukkan melalui implementasi sistem tanda tangan digital untuk verifikasi Surat Permohonan Kuliah Kerja Profesi (KKP) dengan memanfaatkan metode kompresi *Deflate* dan enkripsi *Advanced Encryption Standard (AES)*. Sistem yang dikembangkan mampu menghasilkan mekanisme verifikasi dokumen yang lebih efisien, aman, dan terstruktur dibandingkan dengan proses konvensional yang masih bergantung pada pemeriksaan manual. Integrasi antara proses *preprocessing* data, kompresi, dan enkripsi memungkinkan pengelolaan data surat dilakukan secara optimal tanpa mengurangi keutuhan maupun keabsahan informasi. Selain itu, pemanfaatan *QR Code* sebagai media representasi data terenkripsi mempermudah proses autentikasi dokumen baik dalam bentuk digital maupun cetak. Penyajian hasil penelitian disusun dalam beberapa subbagian utama yang mencerminkan tahapan pengolahan data, mekanisme pengamanan dokumen, serta hasil pengujian fungsional sistem. Dengan demikian, hasil yang diperoleh memberikan gambaran menyeluruh mengenai kinerja, keandalan, dan potensi penerapan sistem dalam mendukung proses verifikasi dokumen akademik yang lebih cepat, aman, dan dapat dipertanggungjawabkan.

3.1 | Implementasi Sistem

Sistem dikembangkan menggunakan Node.js pada sisi server dan React Native pada sisi *client*. Data Surat Permohonan KKP yang telah dikompresi menggunakan metode *Deflate* selanjutnya dienkripsi menggunakan algoritma AES-128-CBC. Hasil enkripsi dikonversi menjadi *QR Code* yang ditempatkan pada dokumen surat sebagai representasi tanda tangan digital.

Gambar 8 memperlihatkan *QR Code* yang dihasilkan dari *Ciphertext* hasil enkripsi AES-128-CBC. *QR Code* berfungsi sebagai representasi visual dari tanda tangan digital yang menyimpan data terenkripsi secara aman. Penggunaan *QR Code* memungkinkan data tanda tangan digital disisipkan pada dokumen digital maupun dicetak secara fisik, serta dapat diverifikasi dengan mudah melalui proses pemindaian. Pada tahap verifikasi, *QR Code* dipindai untuk memperoleh *Ciphertext* yang kemudian didekripsi dan didekompresi guna memastikan keaslian dan keutuhan data surat. Dengan demikian, *QR Code* menjadi komponen utama dalam mekanisme verifikasi tanda tangan digital pada sistem yang dikembangkan.

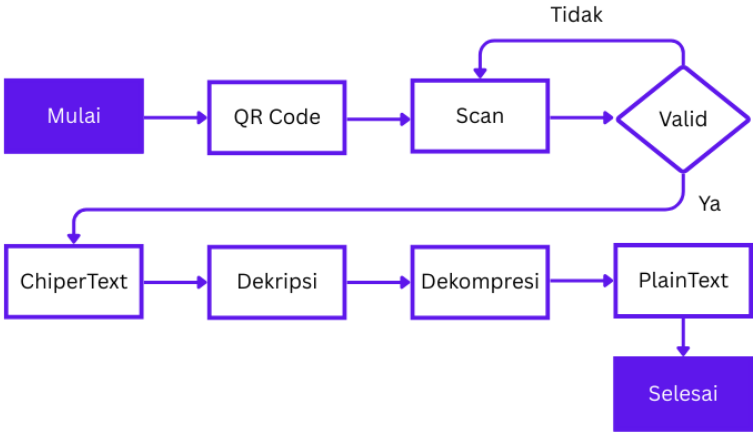
GAMBAR 8 *Output QR Code* Tanda Tangan Digital

3.2 | Analisis Proses Verifikasi

Proses verifikasi dilakukan dengan memindai *QR Code* yang terdapat pada surat menggunakan aplikasi *client*. Data terenkripsi yang diperoleh dari hasil pemindaian kemudian diproses melalui tahap dekripsi menggunakan algoritma AES-128-CBC dan tahap dekompresi menggunakan metode *Deflate*.

Hasil dari proses dekripsi dan dekompresi menunjukkan bahwa data surat dapat dikembalikan ke bentuk semula tanpa perubahan isi. Hal ini membuktikan bahwa integrasi algoritma AES dan metode *Deflate* mampu menjaga integritas dan keaslian data selama proses verifikasi dokumen.

Gambar 9 menunjukkan proses dekripsi dan verifikasi dimulai dengan pengambilan *QR Code* yang telah dihasilkan pada tahap sebelumnya. *QR Code* tersebut kemudian dipindai untuk memperoleh *Ciphertext* yang tersimpan di dalamnya. Setelah proses pemindaian, sistem melakukan validasi untuk memastikan bahwa *QR Code* dan *Ciphertext* yang diperoleh berada dalam format yang valid. Apabila *Ciphertext* tidak valid, proses pemindaian akan diulang hingga data yang sesuai diperoleh. Jika *Ciphertext* dinyatakan valid, sistem melanjutkan ke tahap berikutnya dengan memproses data terenkripsi tersebut. *Ciphertext* kemudian didekripsi menggunakan algoritma AES-128 dengan mode *Cipher Block Chaining (CBC)* untuk menghasilkan *plaintext* dalam bentuk data terkompresi. Selanjutnya, *plaintext* tersebut didekompresi untuk mengembalikan data ke bentuk aslinya. Dengan selesainya tahap dekompresi, data asli Surat Permohonan KKP berhasil diperoleh kembali dan proses verifikasi dinyatakan selesai.



GAMBAR 9 Alur Proses Verifikasi

3.3 | Pengujian Sistem

Pengujian sistem dilakukan menggunakan metode *black-box* untuk memastikan seluruh fungsi berjalan sesuai dengan kebutuhan. Pengujian mencakup proses pembangkitan *QR Code*, pemindaian, dekripsi, dekompresi, serta validasi data surat.

Tabel 1 menunjukkan hasil pengujian fungsional sistem tanda tangan digital menggunakan metode *black-box*. Seluruh fitur utama, mulai dari *preprocessing* data, kompresi *Deflate*, enkripsi AES, hingga proses verifikasi, berhasil dijalankan sesuai dengan spesifikasi yang dirancang. Tidak ditemukan kesalahan fungsional selama proses pengujian, sehingga sistem dinyatakan berjalan dengan baik dan siap digunakan untuk proses verifikasi Surat Permohonan KKP.

TABEL 1 Hasil Pengujian *Black-box*

No.	Kategori Pengujian	Total Test	Berhasil	Gagal	Rata-rata Waktu	Tingkat Keberhasilan	Keterangan Tambahan
1	Kompresi	50	50	0	1.07*ms*	100%	Ukuran berkurang dari 214 menjadi 156 *bytes* (rasio 27.1%), total hemat 2.900 *bytes*
2	Enkripsi	50	50	0	1.88*ms*	100%	Proses enkripsi berhasil tanpa *error*
3	Konversi ke *QR Code*	50	50	0	46.04*ms*	100%	Waktu paling tinggi di antara proses lain karena *rendering QR Code*
4	Validasi *QR Code*	50	50	0	1.07*ms*	100%	Semua QR dapat terbaca dengan benar
5	Dekripsi	50	50	0	1.64*ms*	100%	Semua data kembali ke bentuk asli
6	Dekompresi	50	50	0	0.33*ms*	100%	Data kembali ke ukuran asli (214 *bytes*), valid 100%
7	Validasi Tanda Tangan Digital	50	50	0	0.28*ms*	100%	*Signature* 64 *bytes*, data 500 *bytes*, semua terverifikasi
8	Keamanan	50	34	16	0.87*ms*	68%	Serangan terdeteksi 133/150 (88.7%), hanya 34 sistem bertahan
9	Kecepatan	50	49	1	28.72*ms*	98%	Rata-rata: *Compression* 0.52*ms*, *Encryption* 0.87*ms*, *QR Generation* 27.18*ms*, *Decryption* 0.50*ms*, *Decompression* 0.24*ms*

4 | KESIMPULAN

Perancangan Penelitian ini menyimpulkan bahwa implementasi algoritma *Advanced Encryption Standard (AES)* dan *Deflate* terbukti efektif dalam menjamin keamanan serta keabsahan tanda tangan digital pada dokumen akademik. Melalui proses enkripsi dan dekripsi yang mencapai tingkat keberhasilan 100%, sistem ini mampu menjaga kerahasiaan data dengan sangat baik, sementara penggunaan algoritma *Deflate* berhasil mengoptimalkan efisiensi penyimpanan dengan mereduksi ukuran data rata-rata sebesar ±27%. Kombinasi kedua metode ini memastikan bahwa setiap tanda tangan digital yang dihasilkan bersifat valid, terlindungi integritasnya, dan dapat diverifikasi dengan akurat.

Selain aspek keamanan, aplikasi *mobile* yang dikembangkan telah berhasil mengintegrasikan seluruh proses teknis mulai dari kompresi, enkripsi, hingga konversi ke *QR Code*. Hasil pengujian *black-box* menunjukkan tingkat keberhasilan fungsional rata-rata mencapai 96,2%, yang menegaskan bahwa seluruh fitur utama berjalan sesuai ekspektasi. Keberhasilan pengembangan ini memberikan solusi praktis dalam mempercepat verifikasi Surat Permohonan Kuliah Kerja Profesi (KKP) di Fakultas Teknik UNISMUH Makassar, sekaligus meminimalisir risiko keterlambatan dalam prosedur administrasi akademik.

Secara keseluruhan, penerapan sistem tanda tangan digital ini jauh lebih efektif jika dibandingkan dengan metode verifikasi konvensional. Keunggulan tersebut terlihat dari kecepatan validasi dokumen yang hanya membutuhkan waktu rata-rata 28,72 milidetik dengan tingkat keberhasilan verifikasi yang sempurna. Efisiensi waktu ini membuktikan bahwa sistem digital mampu memberikan jaminan keamanan dan kecepatan yang lebih baik daripada metode manual yang cenderung lambat dan rawan terhadap kesalahan manusia.sekitar.

Daftar Pustaka

Alsaedi, A., & Burnap, P. (2020). Trustworthy digital signatures for secure electronic documents. IEEE Access, 8, 21137–21149. https://doi.org/10.1109/ACCESS.2020.2968889

Arief, M. R., Nugroho, A., & Wibowo, S. (2021). Implementation of AES cryptography for document security systems. Journal of Physics: Conference Series, 1810(1), 012047.

Bansod, G., & Patil, S. (2020). Secure QR code based document authentication using cryptography. International Journal of Advanced Computer Science and Applications, 11(4), 352–358.

Biryukov, A., Perrin, L., & Udovenko, A. (2020). Security analysis of AES-based constructions. IACR Transactions on Symmetric Cryptology, 2020(3), 45–76.

Dey, S., Sampalli, S., & Ye, Q. (2021). A QR-code-based secure document verification system. Sensors, 21(7), 2389.

El Makkaoui, K., Beni-Hssane, A., & Ezzati, A. (2021). A secure digital signature scheme for e-government services. International Journal of Information Security, 20(3), 353–366. https://doi.org/10.1007/s10207-020-00516-4

Fadhil, A., & Hassan, M. (2022). AES encryption performance analysis for secure *mobile* applications. Procedia Computer Science, 197, 152–159.

Fahlevvi, M. R., Putra, D. S. A., & Ariandi, W. (2025). ALGORITMA AES128-CBC (ADVANCED ENCRYPTION STANDARD) UNTUK ENKRIPSI DAN DEKRIPSI BERKAS DOKUMEN PT. ADIARTA MUZIZAT. Journal of Innovation And Future Technology (IFTECH), 7(1), 166-176. https://doi.org/10.47080/iftech.v7i1.3929

Fatma, Y., Fuad, E., & Soni, A. (2023). Aplikasi Tandatangan Digital dalam Proses Verifikasi dan Validasi Sertifikat Covid-19. Techno. Com, 22(1), 134-144. https://doi.org/10.33633/tc.v22i1.7091

Goyal, R., & Purohit, G. N. (2020). Data compression using Deflate algorithm: A performance evaluation. International Journal of Computer Applications, 176(25), 20–25.

Hameed, S., Khan, F., & Hameed, A. (2021). Secure document verification using QR code and cryptographic hash. Future Generation Computer Systems, 118, 1–10.

Hussain, M., & Shah, A. (2022). Digital signature verification for secure document workflows. Journal of Information Security and Applications, 64, 103045. https://doi.org/10.1016/j.jisa.2022.103045

Indriani, R., Ferdiansyah, P., & Koprawi, M. (2024). Analisis Penggunaan Kriptografi Metode AES 256 Bit pada Pengamanan File dengan Berbagai Format. Digital Transformation Technology (Digitech), 4(2), 1245-1251. https://doi.org/10.47709/digitech.v4i2.5457

Kaur, M., & Singh, D. (2021). Hybrid encryption techniques for secure document transmission. Journal of King Saud University – Computer and Information Sciences, 33(7), 820–829.

Kumar, R., & Tripathi, R. (2020). QR code security: Issues and solutions. Computer Communications, 154, 192–205.

Kustyandi, A., & Noor, S. (2021). Sistem informasi monitoring serangan keamanan mail server di Yayasan Assyifa Al-Khoeriyyah. FASILKOM, 8(2), 41–48. https://ejournal.unsub.ac.id/index.php/FASILKOM/article/view/1400

Li, X., Zhang, Y., & Chen, J. (2022). Efficient AES-based encryption for *mobile* document security. *Mobile* Information Systems, 2022, 6843126. https://doi.org/10.1155/2022/6843126

NIST. (2023). Digital Signature Standard (DSS) (FIPS PUB 186-5). https://doi.org/10.6028/NIST.FIPS.186-5

Pemayun, C. T. D., & Dewi, P. E. T. (2025). Keabsahan tanda tangan digital dalam transaksi bisnis [Validity of digital signatures in business transactions]. Jurnal Ilmiah Hukum dan Hak Asasi Manusia (JIHHAM), 4(2), 91–101. https://doi.org/10.35912/jihham.v4i2.3798

Purnama, R., Setiawan, A., & Hidayat, T. (2021). Implementasi tanda tangan digital untuk sistem administrasi akademik. Jurnal RESTI, 5(4), 667–675. https://doi.org/10.29207/resti.v5i4.3267

Rahman, M. A., & Hossain, M. S. (2020). Secure document authentication using cryptographic QR codes. IEEE Access, 8, 145401–145412. https://doi.org/10.1109/ACCESS.2020.3015254

Sari, D. P., & Prasetyo, Y. A. (2022). Pengamanan dokumen digital menggunakan algoritma AES berbasis *mobile*. Jurnal Teknologi Informasi dan Ilmu Komputer, 9(3), 563–570. https://doi.org/10.25126/jtiik.202293567

Sharma, P., & Gupta, B. B. (2021). Digital signature schemes for secure e-documents: A review. Cluster Computing, 24, 2469–2485. https://doi.org/10.1007/s10586-021-03243-8

Sujono, S., Maxrizal, M., & Novianto, D. (2020). Pengelolaan Arsip Secara Digital Menggunakan Algoritma LZSS Modifikasi untuk Kompresi File. JEPIN (Jurnal Edukasi dan Penelitian Informatika), 6(1), 117-121. https://jurnal.untan.ac.id/index.php/jepin/article/view/38301\