# SISTEM PENCATAT KEUANGAN BERBASIS WEB DENGAN ENKRIPSI DAN WATERMARKING MENGGUNAKAN ALGORITMA AES (ADVANCED ENCRYPTION STANDARD

**L. Nurianti[1], Ramadhan Renaldy[2] dan Y. A. Ramadhan[3]**

[1,2,3]*Jurusan Informatika, Fakultas Teknik dan Informatika, Universitas PGRI Semarang*

*Gedung B Lantai 3, Kampus 1 Jl. Sidodadi Timur 24, Semarang (11 pt Italic)*

E-mail : nuriantilucy1@gmail.com [1], ramadhanrenaldy@upgris.ac.id [2], Anandayudha000@gmail.com [3]

***Abstrak***

*Pada masa teknologi yang telah berkembang pesat, sistem transaksi semakin berinofasi dan memudahkan pengguna dalam mengakses, melacak, dan merekap informasi keuangan secara efisien. Namun, kemudahan ini juga membawa tantangan besar terkait dengan ancaman keamanan, khususnya pencurian data dan serangan siber. Informasi keuangan dan data pribadi yang tidak terlindungi dengan baik dapat disalah gunakan oleh pihak yang tidak bertanggung jawab. Oleh karena itu, penting untuk memastikan sistem akuntansi online terlindungi dengan baik, salah satunya melalui penerapan enkripsi. Enkripsi adalah proses mengubah data mentah (plaintext) menjadi bentuk kode yang sulit dimengerti (chipertext), dan hanya dapat dipecahkan menggunakan kunci deskripsi (secret key). Salah satu algoritma cyber scurity adalah algoritma AES (Advanced Encryption Standard). Penelitian ini bertujuan untuk mengembangkan sistem pencatatan keuangan berbasis web yang dilengkapi dengan enkripsi menggunakan algoritma AES untuk melindungi data transaksi dan informasi sensitif pengguna. Penerapan algoritma AES diharapkan dapat meningkatkan keamanan data, mencegah serangan seperti peretasan dan pencurian identitas, serta menjaga integritas data yang tersimpan dalam sistem.*

***Kata Kunci*:** Sistem Keuangan, AES (Advanced Encryption Standard), Watermarking

## I. PENDAHULUAN (10pt huruf besar,rata kiri/bold)

Pada era digital saat ini, proses transaksi keuangan telah berkembang pesat dan berpindah ke sistem berbasis web. Berkembangnya teknologi ini dapat mempermudah pengguna mengakses informasi keuangan, melacak pengeluaran, dan merekap informasi keuangan melalui platform online yang dapat diakses kapan saja dan dimana saja. Namun kemudahan ini juga disertai dengan peningkatan risiko keamanan, terutama terkait pencurian data dan serangan hacker. Informasi keuangan dan data pribadi yang tidak dilindungi dengan baik dapat disalah gunakan oleh pihak yang tidak bertanggung jawab. Oleh karena itu, sangat penting untuk melindungi data keuangan dalam sistem pencatatan keuangan.

Sistem akuntansi online harus terlindungi dengan baik untuk memastikan data pengguna aman dari ancaman seperti peretasan, pencurian identitas, dan manipulasi data (Nizamuddin Aulia Kafa & Dolly Virgian Shaka Yudha Sakti, 2024, p. 1.2). Salah satu cara untuk melindungi data adalah dengan menerapkan enkripsi. Enkripsi adalah sebuah proses pembuatan informasi terkonversi menjadi kode rahasia (Nizamuddin Aulia Kafa & Dolly Virgian Shaka Yudha Sakti, 2024, p. 2). Data yang diterima, dikirim, dan disimpan diubah dengan algoritma. Algoritma yang dipakai digunakan untuk mengacak suatu data, kemudian pihak penerima akan memulihkan kembali data yang teracak tersebut dengan kunci dekripsi (2024, p. 2).

Ekripsi berfungsi untuk mengubah bentuk data menjadi kode (Wijayanto & Wardoyo, 2013, p. 2). Sehingga informasi tersebut hanya dapat diakses oleh pihak yang memiliki kunci dekripsi. Macam-macam enkrisi yaitu, Enkripsi SHA (Secure Hashing Algorithm), Enkripsi Message-Digest Algorithm 2 (MD2), Enkripsi MD4, Enkripsi MD5, Enkripsi Base64, Enkripsi RC4 dan Enkripsi AES. Salah satu metode yang dapat digunakan untuk melindungi data yaitu dengan menerapkan enkrips.



E-ISSN: 2985-3532

Algoritma AES (Advanced Encryption Standard) memiliki tingkat keamanan yang tinggi. AES adalah algoritma enkripsi simetris yang diakui secara luas sebagai standar enkripsi aman (Diaztary et al., 2021, p. 2). Algoritma ini banyak digunakan di berbagai aplikasi dan sistem untuk melindungi data sensitif seperti perbankan online, komunikasi terenkripsi, dan aplikasi keuangan lainnya.

Beberapa penelitian sebelumnya telah menunjukkan keberhasilan penerapan enkripsi AES dalam sistem keuangan. Salah satunya dalam studi Smith et al. (2019), mereka mampu mengurangi kemungkinan serangan man-in-the-middle dan meningkatkan keamanan dengan menerapkan AES pada sistem pencatatan transaksi perbankan (Ahyuna et al., 2021, p. 3). Penelitian lain yang dilakukan Johnson (2021) juga menegaskan bahwa enkripsi AES pada aplikasi pencatatan keuangan berbasis web dapat memberikan perlindungan yang optimal sekaligus menjaga kinerja sistem yang efisien (Sari et al., 2022, p. 2).

Dalam penelitian ini, kami mengembangkan "sistem pencatatan keuangan berbasis web yang dilengkapi dengan enkripsi data menggunakan algoritma AES" berdasarkan permasalahan terkait pengamanan data. Sistem ini dirancang untuk melindungi data keuangan seperti data transaksi, informasi pengguna (Ahyuna et al., 2021, p. 3), dan data sensitif lainnya (Diaztary et al., 2021, p. 2). Penerapan AES diharapkan dapat menjamin kerahasiaan dan integritas data yang disimpan serta melindungi pengguna dari potensi ancaman keamanan.

Watermarking memiliki peran penting dalam melindungi dokumen digital dari pemalsuan atau distribusi tidak sah (Diaztary et al., 2021, p. 2). Dengan menyisipkan informasi unik dalam dokumen (Abdussalam et al., 2019, p. 2), setiap salinan dapat ditelusuri kembali ke sumbernya. Hal ini memberikan lapisan perlindungan tambahan, terutama jika terjadi kebocoran dokumen sensitif. Selain itu, teknik watermarking modern memungkinkan integrasi dengan tanda tangan digital, yang menjamin keaslian dokumen secara hukum (Abdussalam et al., 2019, p. 3).

Dalam konteks sistem keuangan berbasis web, penerapan watermarking juga berfungsi sebagai langkah pencegahan terhadap penyalahgunaan data. Sebagai contoh, jika laporan keuangan didistribusikan tanpa izin, watermark dapat membantu mengidentifikasi sumber kebocoran. Teknologi ini melengkapi enkripsi AES dengan memberikan pengamanan pada level visual dan metadata dokumen, sehingga memberikan solusi keamanan yang komprehensif

## II. METODOLOGI PENELITIAN

### 1. Metodologi Penelitian

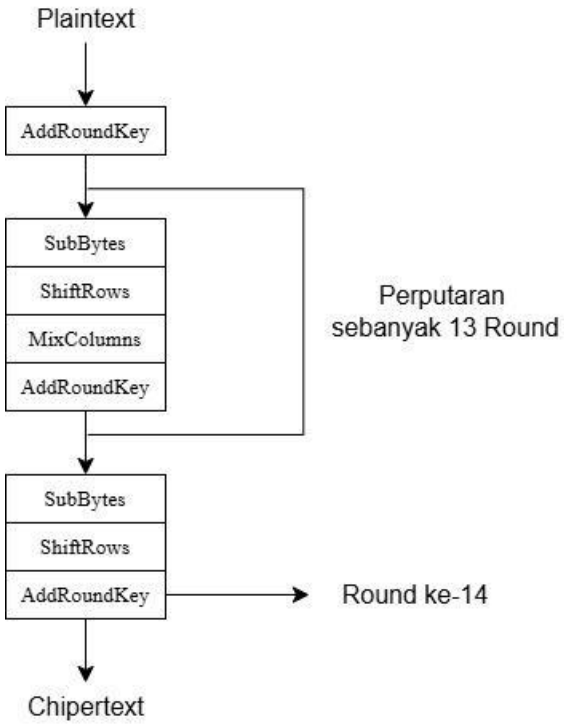
Pada sistem pencatatan keuangan berbasis web ini, metode yang digunakan adalah enkripsi menggunakan Algoritma AES (Advanced Encryption Standard). AES merupakan algoritma kriptografi simetris yang bekerja dengan menggunakan kunci sepanjang 128, 192, atau 256 bit. Algoritma yang digunakan pada sistem ini yaitu algoritma AES 256 bit. Metode ini dipilih karena tingkat keamanan yang tinggi dan efisiensi dalam enkripsi maupun dekripsi data. Data transaksi keuangan pengguna akan dienkripsi sebelum disimpan di dalam basis data, sehingga memastikan hanya pengguna yang memiliki kunci enkripsi yang dapat mengakses informasi asli. Sistem ini dilengkapi watermarking visibel sehingga text logo sistem terlihat jelas pada laporan transaksi yang diproses pada website.

### 2. Proses Enkripsi AES 256Bit

Proses enkripsi AES 256 dimulai dengan melakukan proses AddRoundKey yang terdiri dari 4 proses transformasi, yaitu SubBytes, ShiftRows, MixColumns dan AddRoundKey sebanyak 13 ROUND. Ketika sampai pada Round 14 dilakukan tiga proses transformasi yaitu, SubBytes, ShiftRows, dan AddROUNDKey dan akan menghasilkan cipherteks. Dan akan muncul tampilan hasil enkripsi.



E-ISSN: 2985-3532




Gambar 24. Flowchard Enkripsi AES 256bit

**SubBytes**

**S**ubBytes adalah perubahan penggantian byte secara non-linear yang menggunakan tabel penggantian (S-Box) untuk mengganti setiap byte dalam blok data. Tabel S-Box dirancang berdasarkan transformasi matematika medan Galois ("GF ($2^8$)") untuk menghasilkan penggantian yang tahan terhadap serangan diferensial dan linier.

Table 5.2 AES S-Boxes

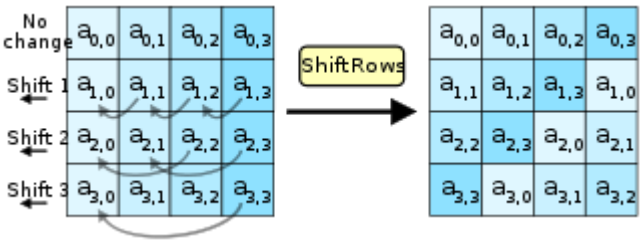
| | | y | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
| x | 0 | 63 | 7C | 77 | 7B | F2 | 6B | 6F | C5 | 30 | 01 | 67 | 2B | FE | D7 | AB | 76 |
| | 1 | CA | 82 | C9 | 7D | FA | 59 | 47 | F0 | AD | D4 | A2 | AF | 9C | A4 | 72 | C0 |
| | 2 | B7 | FD | 93 | 26 | 36 | 3F | F7 | CC | 34 | A5 | E5 | F1 | 71 | D8 | 31 | 15 |
| | 3 | 04 | C7 | 23 | C3 | 18 | 96 | 05 | 9A | 07 | 12 | 80 | E2 | EB | 27 | B2 | 75 |
| | 4 | 09 | 83 | 2C | 1A | 1B | 6E | 5A | A0 | 52 | 3B | D6 | B3 | 29 | E3 | 2F | 84 |
| | 5 | 53 | D1 | 00 | ED | 20 | FC | B1 | 5B | 6A | CB | BE | 39 | 4A | 4C | 58 | CF |
| | 6 | D0 | EF | AA | FB | 43 | 4D | 33 | 85 | 45 | F9 | 02 | 7F | 50 | 3C | 9F | A8 |
| | 7 | 51 | A3 | 40 | 8F | 92 | 9D | 38 | F5 | BC | B6 | DA | 21 | 10 | FF | F3 | D2 |
| | 8 | CD | 0C | 13 | EC | 5F | 97 | 44 | 17 | C4 | A7 | 7E | 3D | 64 | 5D | 19 | 73 |
| | 9 | 60 | 81 | 4F | DC | 22 | 2A | 90 | 88 | 46 | EE | B8 | 14 | DE | 5E | 0B | DB |
| | A | E0 | 32 | 3A | 0A | 49 | 06 | 24 | 5C | C2 | D3 | AC | 62 | 91 | 95 | E4 | 79 |
| | B | E7 | C8 | 37 | 6D | 8D | D5 | 4E | A9 | 6C | 56 | F4 | EA | 65 | 7A | AE | 08 |
| | C | BA | 78 | 25 | 2E | 1C | A6 | B4 | C6 | E8 | DD | 74 | 1F | 4B | BD | 8B | 8A |
| | D | 70 | 3E | B5 | 66 | 48 | 03 | F6 | 0E | 61 | 35 | 57 | B9 | 86 | C1 | 1D | 9E |
| | E | E1 | F8 | 98 | 11 | 69 | D9 | 8E | 94 | 9B | 1E | 87 | E9 | CE | 55 | 28 | DF |
| | F | 8C | A1 | 89 | 0D | BF | E6 | 42 | 68 | 41 | 99 | 2D | 0F | B0 | 54 | BB | 16 |

**(a) S-box**

Gambar 2. Tabel S-box

**ShiftRows**

ShiftRows adalah proses pergeseran satu baris dalam blok setiap byte, pergeseran dimulai dari byte kiri kemudian dipindahkan ke byte kanan. Proses pergeseran byte dapat dilihat pada Gambar 2.1.1 Tabel S-box.




Gambar 3. Perpindahan shiftRows

**MixColumns**

MixColumns adalah proses pengoprasian setiap element dalam satu kolom state berukuran 4x4, Proses MixColumns menggunakan operasi matriks atas elemen-elemen dalam Golois *GF* ($2^8$).

$$s'(x) = a(x) \otimes s(x)$$

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

$$s'_{0,c} = (\{02\} \bullet s_{0,c}) \oplus (\{03\} \bullet s_{1,c}) \oplus s_{2,c} \oplus s_{3,c}$$

$$s'_{1,c} = s_{0,c} \oplus (\{02\} \bullet s_{1,c}) \oplus (\{03\} \bullet s_{2,c}) \oplus s_{3,c}$$

$$s'_{2,c} = s_{0,c} \oplus s_{1,c} \oplus (\{02\} \bullet s_{1,c}) \oplus (\{03\} \bullet s_{3,c})$$

$$s'_{3,c} = (\{03\} \bullet s_{0,c}) \oplus s_{0,c} \oplus s_{1,c} \oplus (\{02\} \bullet s_{3,c})$$

Gambar 4. Perkalian Matriks pada MixColumns

**AddRoundKey**

AddRoundKey adalah proses menggabungkan plaintext atau chipertext dengan kunci engkripsi. sebuah round key ditembahkan pada state menggunakan oprasi XOR.

## 3. Proses Deskripsi AES 256Bit

Transformasi kriptografi bersifat reversibel dan diimplementasikan dalam arah yang berlawanan untuk menghasilkan cipher invers yang mudah dipahami untuk algoritma AES. Transformasi byte yang digunakan dalam cipher terbalik adalah InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey.

## 4. Penerapan Watermarking

Watermarking diterapkan pada laporan keuangan yang dihasilkan sistem untuk melindungi keaslian dokumen digital. Proses ini melibatkan:



E-ISSN: 2985-3532

1. **Pembuatan Watermark:**
    - Sistem menghasilkan watermark berupa informasi unik pengguna, seperti ID pengguna dan tanggal pembuatan laporan.
    - Watermark ditambahkan ke dalam laporan dalam format PDF menggunakan library DomPDF.
2. **Integrasi Watermark:**
    - Watermark disematkan sebagai lapisan transparan pada dokumen PDF.
    - Proses ini memastikan watermark tidak mudah dihapus atau diubah tanpa meninggalkan jejak digital.

Kode PHP untuk watermarking:

```
use Dompdf\\Dompdf;

function generateWatermarkedPDF($content, $watermarkText) {
    $dompdf = new Dompdf();
    $dompdf->loadHtml($content);

    // Tambahkan watermark
    $canvas = $dompdf->getCanvas();
    $canvas->page_script(function ($canvas) use ($watermarkText) {
        $canvas->set_opacity(0.3);
        $canvas->text(150, 400, $watermarkText, null, 50, [0.85, 0.85, 0.85]);
    });

    $dompdf->render();
    return $dompdf->output();
}
```


Gambar 5. Flowchard Sistem

## 5. Alur Sistem

Alur dari sistem pencatatan keuangan ini dimulai ketika pengguna melakukan login ke dalam sistem menggunakan username dan password. Password yang di inputkan kemudian diengkripsi menggunakan algoritma AES-256bit. Jika username dan password valid maka pengguna diarahkan ke Dashboard yang menampilkan ringkasan keuangan mereka dan menyediakan opsi untuk menambah kategori pemasukan dan pengeluaran serta jumlah nominalnya atau melihat riwayat transaksi yang sudah ada.

Ketika pengguna ingin melihat transaksi yang telah dicatat, sistem akan mengambil data yang telah disimpan pada database. Setelah pengguna selesai, mereka dapat mencetak laporan keuangannya dengan format file pdf dan dapat didonwload serta disimpan pada perangkat pengguna. Pada file yang didonwload terdapat watermark yang dapat digunakan untuk melindungi informasi sensitif pada dokumen keuangan dengan menandai bahwa dokumen tersebut bersifat rahasia atau terbatas.

Alur sistem secara keseluruhan dapat digambarkan sebagai berikut:

- Pengguna memasukkan data login yang nantinya di engkripsi menggunakan alotitma AES 256bit



E-ISSN: 2985-3532

- Pengguna dapat memasukkan data keuangan yang akan disimpan dalam basis data.
- Pengguna dapat mencetak laporan dengan watermark untuk melindungi informasi sensitif pada dokumen keuangan

## 6. Kebutuhan Sistem

Sistem terdiri atas tiga komponen utama:

- **Frontend:** Antarmuka pengguna dikembangkan menggunakan framework Bootstrap dan Vue.js untuk memudahkan interaksi pengguna dengan sistem.
- **Backend:** Server aplikasi dibangun menggunakan PHP dengan framework Laravel yang menyediakan fitur keamanan bawaan, seperti hashing kata sandi dan middleware untuk otorisasi.
- **Database:** Data keuangan disimpan pada basis data MySQL yang diintegrasikan dengan Laravel melalui Eloquent ORM

## III. HASIL DAN PEMBAHASAN

.Pengujian sistem dilakukan untuk memastikan keamanan dan kinerja fitur yang dikembangkan. Metode pengujian meliputi:

- **Pengujian Enkripsi dan Dekripsi:** Memastikan data terenkripsi dengan benar dan dapat didekripsi tanpa kehilangan informasi.
- **Pengujian Watermarking:** Memastikan watermark tampil pada laporan PDF dan sulit dihapus.
- **Pengujian Kinerja:** Mengukur waktu yang diperlukan untuk enkripsi, dekripsi, dan pembuatan laporan ber-watermark.

### Analisis Keamanan

Untuk menguji tingkat keamanan, analisis dilakukan dengan mengukur:

- **Ketahanan Enkripsi:** Pengujian brute force pada algoritma AES untuk memastikan kunci enkripsi sulit ditebak.
- **Integritas Watermarking:** Menguji kemampuan watermark bertahan terhadap modifikasi file PDF.

### Hasil Engkripsi AES

Berikut hasil enkripsi password menggunakan algoritma AES (Advanced Encryption Standard) 256bit dengan plaintext “eka123” dengan enkripsi AES didapatkan chipertext

“AUm5Z8mGP01cV1J5ydKba0WxYQ1hiVFZSZDRaa25K0G1kZjVVa1E9PQ”

### Hasil Cetak Laporan Semua Transaksi Format PDF Dengan Watermark

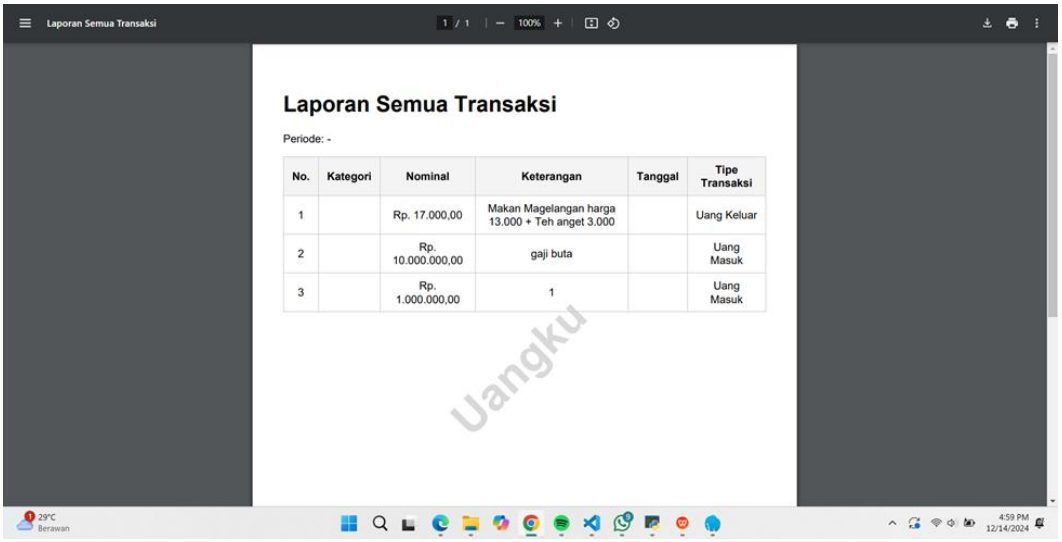
Fitur download laporan dalam format PDF adalah salah satu fitur utama dalam aplikasi ini. Setelah pengguna memilih rentang tanggal yang diinginkan dan melihat rincian transaksi, mereka dapat mengunduh laporan tersebut dalam format PDF yang telah dilengkapi dengan watermark "Uangku".



E-ISSN: 2985-3532

Proses pengunduhan laporan PDF berfungsi sebagai sarana untuk menyimpan dan mencetak laporan keuangan secara fisik atau digital. Fitur ini sangat berguna untuk keperluan arsip atau pelaporan kepada pihak ketiga. Dalam file PDF yang diunduh, selain data transaksi seperti nomor, kategori, nominal, keterangan, tanggal, dan tipe transaksi, watermark "Uangku" akan ditampilkan di setiap halaman laporan.

Pengguna cukup menekan tombol Download Laporan pada halaman laporan transaksi untuk mengunduh file PDF yang sudah diproses dengan watermarking dan siap digunakan.



Gambar 6. Laporan Semua Transaksi format pdf dengan watermak

## IV. KESIMPULAN

Berdasarkan hasil implementasi dan pengujian sistem Pencatatan Keuangan Berbasis Web dengan Enkripsi dan Watermarking Menggunakan Algoritma AES dapat disimpulkan, penggunaan metode AES (Advanced Encryption Standard) 256bit memiliki tingkat keamanan yang tinggi. Penerapan Engkripsi AES 256bit dalam fitur login pada bagian password dapat memastikan pengguna akan aman dari potensi ancaman serangan brute force. Hal ini disebabkan karena algoritma AES memiliki 4 proses transformasi, yaitu SubBytes, ShiftRows, MixColumns dan AddRoundKey yang dilakukan sebanyak 14 putaran yang menjadikan algoritma ini sangat cocok untuk melindungi data transaksi didalam sistem pencatat keuangan.

Sistem ini juga menerapkan fitur watermarking visibel pada laporan transaksi yang diunduh dalam format PDF. Watermark bertuliskan "Uangku" yang disisipkan pada setiap halaman laporan untuk menandakan keaslian dan sumber laporan tersebut. Hal ini memberikan perlindungan tambahan terhadap dokumen, memastikan bahwa laporan yang diunduh atau dicetak berasal dari aplikasi yang sah dan tidak dapat dimanipulasi tanpa terdeteksi.

## V. REFERENSI

Abdussalam, A., Hari Rachmawanto, E., Noor, A. S., Ignatius Moses Setiadi, D. R., & Atika Sari, C. (2019). Optimasi Keamanan Watermarking pada Daubechies Transform Berbasis Arnold Cat Map. *Jurnal Informatika: Jurnal Pengembangan IT*, *4*(1), 31–37. https://doi.org/10.30591/jpit.v4i1.911

Akbar, Z. (2010, April 19). *Watermarking Java Programs using Dummy Methods with Dynamically Opaque Predicates*. arXiv.Org. https://arxiv.org/abs/1004.3250

Basaruddin, T., & Maulidiya, D. (2010). KINERJA SKEMA PEMBERIAN TANDA AIR VIDEO DIJITAL BERBASIS DWT-SVD DENGAN DETEKTOR SEMI-BLIND. *MAKARA of Technology Series*, *13*(1). https://doi.org/10.7454/mst.v13i1.489

Diaztary, W., Atmajaya, D., Umar, F., Purnawansyah, Harlinda, & Abdullah, S. M. (2021). Tiny encryption algorithm on discrete cosine transform watermarking. *2021 3rd East Indonesia Conference on Computer and Information Technology (EIConCIT)*, 415–420. https://doi.org/10.1109/eiconcit50028.2021.9431930

Nizamuddin Aulia Kafa, & Dolly Virgian Shaka Yudha Sakti. (2024). Implementasi Kriptografi Berbasis Web dengan Algoritma Advanced Encryption Standard (AES) 256 dan Kompresi Huffman untuk Pengamanan File di SMK Satria. *Jurnal Ticom: Technology of Information and Communication*, *12*(2), 50–55. https://doi.org/10.70309/ticom.v12i2.109

Sari, M., Purnomo, H. D., & Sembiring, I. (2022). Review: Algoritma Kriptografi Sistem Keamanan SMS di Android. *Journal of Information Technology*, *2*(1), 11–15. https://doi.org/10.46229/jifotech.v2i1.292

Wijayanto, B., & Wardoyo, R. (2013). An implementation of catmap-rijndael (AES) algorithm for image security (case study on A software for making students card at universitas jenderal soedirman). *IJCCS (Indonesian Journal of Computing and Cybernetics Systems)*, *5*(2). https://doi.org/10.22146/ijccs.1995

(2021). *Journal of Computer System and Informatics (JoSYC)*, *3*(1). https://doi.org/10.47065/josyc.v3i1



E-ISSN: 2985-3532