PERANCANGAN DAN EVALUASI PROTOKOL KEAMANAN UNTUK IJAZAH DENGAN INTEGRASI DIGITAL WATERMARKING BERBASIS AES-128 DAN ANALISIS FORENSIK STATIS

Muhamad Firmansyah[1], Rizky Rahman Judie Putra[2], Eddy Prasetyo Nugroho[3]
Universitas Pendidikan Indonesia[123]
Jalan Dr.Setiabudi No.229, Bandung, Jawa Barat, 40154
E-mail: firmann19@upi.edu[1], rizky_rjp@upi.edu[2], eddypn@upi.edu [3]

ABSTRAK

Dokumen ijazah pendidikan tinggi merupakan dokumen resmi yang sangat penting dan sering menjadi sasaran pemalsuan atau penyalahgunaan. Dalam era digital, tantangan terhadap keaslian dan integritas dokumen digital semakin kompleks, sehingga diperlukan mekanisme keamanan yang kuat untuk menghindari pemalsuan dan penyalahgunaan. Penelitian ini bertujuan untuk merancang dan mengevaluasi protokol keamanan dokumen digital ijazah dengan mengintegrasikan teknik digital watermarking dan metode analisis statis digital forensik yang dibantu dengan kriptografi dan steganografi. Kriptografi yang digunakan dalam penelitian ini adalah algoritma AES-128 dengan mode CBC, yang berfungsi untuk mengenkripsi dan mendekripsi informasi watermark sebelum disisipkan ke dalam dokumen. Selanjutnya watermark berisi informasi autentikasi yang terenkripsi akan disisipkan ke dalam dokumen digital ijazah, yang nantinya akan dipakai sebagai identifikasi dokumen digital ijazah. Kemudian melakukan analisis forensik statis untuk mendeteksi dan mengidentifikasi potensi modifikasi atau manipulasi digital. Evaluasi dilakukan terhadap tingkat keberhasilan deteksi manipulasi, keakuratan identifikasi keaslian dokumen, serta ketahanan watermark terhadap berbagai serangan digital, dengan menguji terhadap tiga aspek utama yaitu robustness, imperceptibility, dan capacity. Hasil penelitian menunjukkan bahwa integrasi kedua pendekatan ini mampu meningkatkan perlindungan dokumen ijazah, dengan menggunakan empat skenario: (1) dokumen ijazah asli, (2) dokumen ijazah hasil manipulasi, (3) dokumen ijazah hasil scan ulang, dan (4) dokumen ijazah asli yang diduplikasi. Protokol ini diharapkan dapat menjadi solusi keamanan dokumen yang andal dalam sistem administrasi pendidikan digital.

Kata kunci: Protokol Keamanan, Ijazah Digital, Digital Watermarking, Analisis Statis, Digital Forensik.

ABSTRACT

Higher education diplomas are critical official documents that are often subject to forgery and misuse. In the digital era, ensuring the authenticity and integrity of such documents presents increasing challenges, requiring robust security mechanisms. This paper proposes a security protocol for digital diploma documents by integrating digital watermarking and static digital forensic analysis, supported by cryptography and steganography. The watermark contains encrypted authentication information using the AES-128 algorithm in CBC mode, which is embedded into the digital document and serves as its identifier. A static forensic analysis is then applied to detect and identify potential modifications or tampering. The proposed method is evaluated based on its manipulation detection success rate, authenticity verification accuracy, and watermark resilience, tested through three primary metrics: robustness, imperceptibility, and capacity. The protocol is validated through four scenarios: (1) original diploma document, (2) manipulated document, (3) re-scanned document, and (4) duplicated original document. Experimental results demonstrate that the integration of watermarking and forensic techniques enhances document protection, offering a reliable solution for securing digital diploma documents within academic administrative systems.

Keywords : *Security Protocol, Security Information, Diploma Document, Digital Watermarking, Static Analysis, Digital Forensics.*

1. PENDAHULUAN

Kemajuan teknologi informasi saat ini telah mengalami pertumbuhan yang cepat dan memberikan dampak positif dengan peningkatan produktivitas dan efisiensi dalam aktivitas sehari-hari manusia. Dalam hal tersebut, transaksi data juga telah menjadi bagian yang tak terpisahkan dari kehidupan sehari-hari. Transaksi data merujuk pada pertukaran, penyimpanan, dan pengolahan informasi melalui berbagai saluran elektronik [1]. Hal tersebut berlaku juga terhadap dokumen, yang dulunya terkait erat dengan bentuk fisik, kini sering kali diwakili dalam bentuk digital, memudahkan akses dan distribusi global [2].

Dengan perkembangan teknologi saat ini, penerbitan dokumen ijazah sering menggunakan dokumen yang sudah di scan berbentuk digital dengan format Portable Document Format (PDF), format PDF dipilih karena bersifat universal, mudah diakses, dan mampu mempertahankan tata letak dokumen seperti aslinya. Namun, PDF juga dapat dengan mudah disalin, disimpan, dan didistribusikan kembali [3].

Dampak yang bisa terjadi dalam hal ini adalah pemalsuan dokumen ijazah. Pemalsuan dokumen melibatkan tindakan ilegal seperti memanipulasi informasi yang dapat disalahgunakan untuk tujuan yang merugikan, seperti penipuan identitas atau penipuan lainnya untuk memperoleh keuntungan yang tidak semestinya. Di sisi lain, pemalsuan dokumen ijazah digital semakin canggih, mengancam integritas dan validitas informasi yang terdapat dalam dokumen tersebut [4].

Dari ancaman tersebut, perlu adanya upaya untuk memverifikasi dokumen yang efisien dan dapat diandalkan yang berguna untuk menentukan apakah dokumen yang sedang dipertimbangkan sudah dimanipulasi atau tidak, Hal ini dibutuhkan karena dokumen resmi biasanya memiliki karakteristik dan sifat yang resmi yang dapat diidentifikasi [5].

Dalam hal ini, upaya yang dimaksud adalah dengan membuat protokol keamanan. Untuk membangun protokol keamanan, diperlukan beberapa metode atau algoritma yang mendukung. Pada penelitian ini, protokol keamanan dokumen yang dibuat akan menggunakan algoritma digital watermarking dan metode analisis statis.

Digital watermarking digunakan untuk mengatasi masalah kerahasiaan (*Confidentiality*) dan autentikasi (*Authentication*) pada aspek kemananan informasi, di mana pada saat proses penyisipan watermark, watermark akan diberikan enkripsi menggunakan Algoritma AES-128 dengan metode CBC, lalu diberikan sebuah kunci yang tidak dapat diakses oleh pihak yang tidak terdaftar [6]. Selain itu, metode watermarking juga memuat informasi identitas pemilik, seperti nama individu atau instansi terkait, sehingga apabila terjadi manipulasi atau pemalsuan data pada dokumen, watermark dapat menjadi bukti keaslian informasi. Dengan demikian, digital watermarking dapat berfungsi sebagai penjamin keaslian dan kepemilikan dokumen digital [7].

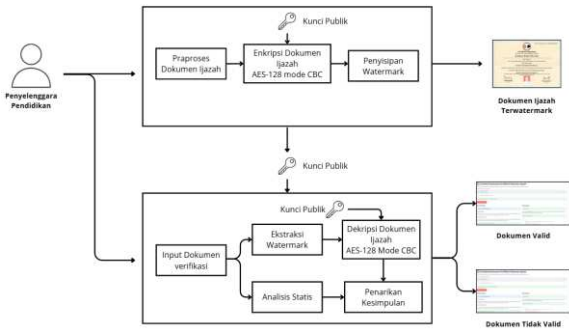
Metode Analisis Statis akan digunakan untuk penguatan aspek pada integritas data. Integritas data menjadi sangat krusial, terutama ketika dokumen mengalami perpindahan atau penyimpanan yang rentan terhadap perubahan yang tidak sah, yang berpotensi mengubah isi dokumen tanpa terdeteksi [8]. Analisis stasis memungkinkan pemeriksaan terhadap struktur internal dokumen secara menyeluruh dengan cara menganalisis representasi biner atau sintaks dari file tersebut. Mengidentifikasi alat atau toolkit yang digunakan untuk membuat file PDF atau mencari asal usul PDF berdasarkan metadata file dokumen, serta dapat mengidentifikasi pola struktur internal file yang dianggap sudah dimanipulasi [9].

Dari berbagai penelitian mengenai digital watermark [10], [11], [12] dan metode analisis statis [13], [14]. Menunjukkan bahwa kedua metode ini bisa diintegrasikan untuk mendapatkan tingkat keamanan data yang lebih baik. Selanjutnya, penelitian-penelitian sebelumnya berfokus pada aplikasi di domain citra sederhana atau media citra pada umumnya, yang belum mengeksplorasi secara spesifik penggunaan watermark kriptografis pada dokumen digital formal seperti ijazah pendidikan tinggi. Selain itu, penelitian terdahulu cenderung menerapkan watermark statis sederhana tanpa mengombinasikannya secara sistematis dengan pendekatan keamanannya melalui algoritma simetris seperti AES□128.

Dalam konteks pengujian penelitian sebelumnya belum ada yang melakukan evaluasi ketahanan watermark pada real world scenario seperti: manipulasi dokumen, re-scan, atau duplikasi. Studi yang ada jarang menguji sekaligus tiga aspek utama dalam keamanan yaitu: *robustness*, *imperceptibility*, dan *capacity*.

2. METODE PENELITIAN

2.1. Arsitektur Sistem



Gambar 2.1 Arsitektur Sistem

Sistem keamanan dokumen ijazah digital ini mengimplementasikan dua tahapan utama yaitu proses pembuatan dokumen ijazah dan proses verifikasi dokumen ijazah.

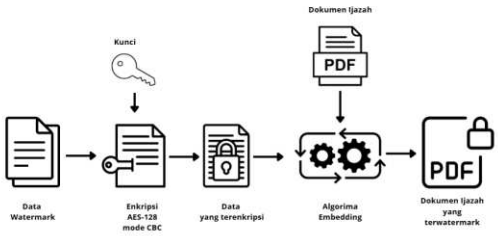
Pada tahap pembuatan dokumen ijazah, lembaga pendidikan sebagai pihak yang berwenang untuk memulai proses dengan pembuatan dokumen ijazah dalam bentuk fisik (*hardcopy*). Dokumen ini kemudian didigitalisasi melalui proses pemindaian (*scanning*) untuk menghasilkan bentuk dokumen dengan format digital dengan file format PDF. Sebelum melakukan proses penyisipan watermarking, Lembaga pendidikan akan menetapkan sebuah kunci rahasia (secret key) yang akan digunakan untuk enkripsi dan digunakan untuk tahap verifikasi di kemudian hari. Selanjutnya, data watermark digital disisipkan ke dalam dokumen digital menggunakan kunci tersebut. Setelah proses ini selesai, dokumen ijazah digital yang telah diberi watermark siap untuk didistribusikan kepada pemegang hak.

Pada tahap verifikasi, keaslian dokumen diuji melalui pendekatan yang mengintegrasikan ekstraksi watermark pada dokumen digital dan analisis statis. Proses ini dimulai ketika sebuah dokumen ijazah yang ingin diverifikasi diberikan kembali ke lembaga pendidikan untuk divalidasi. Langkah yang pertama yaitu melakukan proses ekstraksi watermark dari dokumen yang diberikan, kemudian setelah diekstraksi maka akan melakukan proses dekripsi dengan menggunakan kunci rahasia yang identik pada saat digunakan dalam enkripsi watermark. Tujuan dari langkah ini adalah untuk mendeteksi adanya watermark pada dokumen ijazah. Selanjutnya, dokumen tersebut juga melalui proses analisis statis yang memeriksa anomali pada metadata dan struktur internal file PDF. Hasil dari kedua analisis ekstraksi watermark dan analisis statis akan digunakan untuk menghasilkan keputusan final mengenai otentisitas dokumen, apakah asli atau telah dimodifikasi.

2.2 Digital Watermarking

Digital Watermarking merupakan metode untuk menyisipkan suatu informasi pada suatu data digital dengan tujuan untuk perlindungan kepemilikan dari data tersebut [15]. Metode ini merupakan suatu bentuk dari Steganography (Ilmu yang mempelajari teknik-teknik untuk menyembunyikan keberadaan pesan sekunder di tengah-tengah keberadaan pesan utama) [16]. Oleh karena itu, metode ini sulit dilihat oleh indera manusia tanpa alat bantuan seperti komputer, dan sejenisnya.

2.2.1. Proses Embedding



Gambar 2.2 Proses Embedding Digital Watermarking

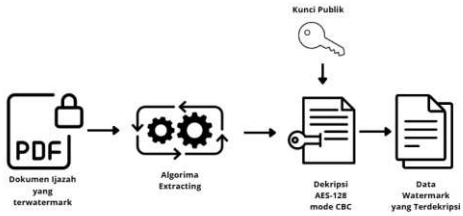
Pada sistem ini data watermark akan dienkripsi dan didekripsi dengan kunci publik yang dibuat sebelumnya menggunakan algoritma AES-128 mode CBC [17], hal ini bertujuan untuk melindungi informasi didalam watermark. Kemudian pada tahap embedding nantinya akan dilakukan penyisipan kedalam metadata PDF dan juga pada content stream pada PDF. *Content stream* merupakan nilai yang terdapat pada sebuah file yang memiliki format PDF, nilai tersebut dapat mempresentasikan semua objek yang terdapat pada sebuah file PDF [18]. Nilai *content stream* dalam gambar 2.3 dimuat dari awalan baris *stream* hingga *endstream*.

P-ISSN: 2337-8344
E-ISSN: 2623-1247

```
7 0 obj
   << /Length 8 0 R >>                    % An indirect reference to object 8
stream
   BT
      /F1 12 Tf
      72 712 Td
      (A stream with an indirect length) Tj
   ET
endstream
endobj
8 0 obj
   77                                     % The length of the preceding stream
endobj
```

Gambar 2.3 Struktur *Content Stream* pada PDF

2.2.2. Proses *Extracting*



Gambar 2.4 Proses *Extracting* Digital Watermarking

Pada tahap *extracting* lakukan proses dengan kebalikan dari *embedding*, tahap pertama yaitu dengan melakukan *Extracting* pada kedua tempat yang disisipkan sebelumnya, yaitu pada metadata PDF dan content stream pada PDF. Selanjutnya nilai watermark yang didapatkan pada kedua penyisipan tersebut nantinya akan melalui proses dekripsi dengan algorima dan kunci publik yang sama pada proses *embedding*. Hasil tersebut nantinya akan dibandingkan untuk bukti validasi bahwa dokumen tersebut asli dan bukan merupakan dokumen modifikasi.

2.3. Analisis Statis

Analisis Statis adalah proses dimana data akan diperiksa tanpa menjalankan programnya secara langsung, dengan tujuan untuk mendapatkan data struktur dari sumber program tersebut. Contohnya seperti menganalisis isi dari sebuah hard disk, metadata sebuah file, dan data data yang bersifat diam [19].

Dalam penelitian ini, metode analisis statis akan digunakan terhadap dokumen ijazah yang memiliki format PDF, hal ini dilakukan pada proses pemeriksaan file tanpa membuka atau menjalankan isinya secara aktif. Analisis yang akan dilakukan adalah dengan menganalisis dan mengidentifikasi karakteristik struktur file PDF, metadata tersembunyi, atau perangkat lunak (tool) yang digunakan untuk menghasilkan dokumen tersebut.

2.3.1. Analisis Metadata

Proses ini akan menganalisis metadata yang terdapat pada PDF menggunakan aplikasi bantuan *Exiftool*. Analisis ini berfokus pada pencarian ketidakwajaran atau keanehan yang sering terdapat pada dokumen yang telah dimanipulasi. Metode ini bekerja seperti investigasi digital, mengungkap "sidik jari" yang ditinggalkan oleh setiap perangkat lunak yang berinteraksi dengan dokumen tersebut [20].

2.3.1. Analisis Struktur PDF

Selain analisis metadata, tahap verifikasi dalam metode analisis statis adalah pemeriksaan dan analisis terhadap struktur internal dokumen PDF itu sendiri. Pendekatan ini bekerja dengan membuat "sidik jari struktural" (structural signature) untuk setiap dokumen [9].

```
Catalog, Pages, Page, Font, FontDescriptor, Metadata
```

Gambar 2.5 *Structural Signature* pada PDF

Metode ini didasarkan pada fakta bahwa setiap perangkat lunak yang membuat atau memodifikasi file PDF akan menyusun objek-objek internalnya (seperti halaman, gambar, dan font) dengan caranya sendiri [21].

2.4. Metode Pengujian

Dalam memvalidasi efektifitas dari seluruh protokol keamanan yang akan dikembangkan, sebuah pengujian yang sistematis akan dilakukan. Pengujian ini dirancang untuk mengevaluasi sistem dari setiap komponen protokol yaitu, digital watermarking dan analisis statis dalam menghadapi berbagai skenario penggunaan yang akan dilakukan. Evaluasi akan dilakukan menggunakan empat skenario dokumen yang berbeda yang akan mempresentasikan kasus penggunaan pada dunia nyata.

- **Dokumen Asli:** Dokumen Ijazah yang telah diberi watermark sesuai protokol keamanan yang digunakan. Dokumen ini digunakan sebagai thershold atau acuan untuk memastikan sistem dapat mengenali dokumen yang resmi dibuat.
- **Dokumen Modifikasi:** Dokumen ijazah asli yang konten visualnya akan dirubah

menggunakan aplikasi editor sepert Adobe Acrobat [22] Skenario dibuat dengan tujuan untuk menguji kemampuan protokol dalam mengidentifikasi manipulasi dokumen ijazah.

- **Dokumen Hasil Scan Ulang:** Dokumen Asli yang dicetak ulang menjadi sebuah media fisik kemudian dibuat kembali menggunakan scanner menjadi sebuah file PDF baru. Skenario ini akan mensimulasikan upaya pemalsuan dengan mencoba menscan ulang
- **Dokumen Asli yang Diduplikasi:** Salinan file langsung dari dokumen ijazah asli yang telah ter watermark. Skenario ini akan membuktikan apakah nilai duplikasi termasuk kedalam dokumen yang asli atau tidak dalam protokol keamanan ini.

Selanjutnya dalam keempat skenario tersebut, kinerja digital watermarking juga akan dievaluasi menggunakan tiga parameter kunci seperti yang disebutkan pada penelitan [23] yaitu:

- ***Robustness***: *Robustness* berarti parameter mengenai ketahanan, dalam konteks ini pengujian dilakukan dengan mencoba mengekstrak watermark dari setiap skenario dokumen. Keberhasilan deteksi dinilai dari hasil ekstraksi secara utuh pada dokumen yang dimodifikasi atau discan ulang.
- ***Imperceptibility***: Parameter ini mengevaluasi digital watermarking menggunakan perbandingan visual antara dokumen sebelum dan sesudah penyisipan watermark untuk memastikan perubahan konten visual yang terlihat langsung oleh mata manusia.
- ***Capacity***: Paramater yang menganalisis penambahan ukuran file setelah proses watermarking. Pengujian ini dilakukan pada 10 sampel dokumen untuk menghitung rata-rata persentase penambahan ukuran, guna memastikan protokol tetap efisien.

Metode analisis statis juga diterapkan pada keempat skenario untuk menganalisis pada metadata dan struktur internal PDF, yang kemudian hasilnya akan dibandingkan untuk memberikan putusan akhir mengenai keaslian dan integritas setiap dokumen ijazah digital.

3. HASIL DAN PEMBAHASAN

Bagian ini memuat pembahasan mengenai hasil dari digital watermarking dan analisis statis yang dilakukan pada dokumen ijazah pendidikan tinggi.

3.1. Kinerja Protokol pada Digital Watermarking

Penelitian ini akan mengevaluasi tiga parameter pada kinerja digital watermarking.

3.1.1. *Robustness*

Untuk menguji *Robustness* diperlukan empat skenario dokumen dengan bantuan media PDF editor dan juga alat *scanner* untuk menganalisis apakah watermark yang disisipkan tahan terhadap sebuah perubahan pada file. Hasil tersebut dijelaskan pada tabel 1 dibawah ini.

Tabel 1. Hasil Ekstraksi pada Dokumen Ijazah

Dokumen Ijazah PDF	Metadata	*Content Stream*	Keterangan
Ijazah watermark asli	Berhasil	Berhasil	Dokumen asli, watermark terdeteksi utuh, maka dinyatakan valid
Ijazah hasil modifikasi	Berhasil	Gagal	Dokumen modifikasi, hasil watermak pada metadata dan pada tampilan gambar berbeda, maka dinyatakan tidak valid
Ijazah Scan ulang	Gagal	Gagal	Dokumen asli dengan scan yang berbeda, watermark tidak terdeteksi, maka dinyatakan tidak valid
Ijazah Asli yang diduplikasi	Berhasil	Berhasil	Dokumen asli, watermark terdeteksi utuh, maka dinyatakan valid

Pengujian *robustness* menunjukkan adanya sifat *fragile* yang dibuat dari proses *watermarking*. Pada skenario dokumen asli dan duplikasi, *watermark* berhasil diekstraksi dari kedua

P-ISSN: 2337-8344
E-ISSN: 2623-1247

tempat penyisipan. Namun, pada skenario dokumen modifikasi, ekstraksi dari *content stream* gagal total karena modifikasi dengan PDF editor akan merusak struktur objek dengan aturannya masing-masing. Pada skenario scan ulang, ekstraksi gagal total dari kedua lokasi. Pada akhirnya watermark akan rusak jika dilakukan proses modifikasi atau hasil scan ulang.

3.1.2. *Imperceptibility*

Hasil pengujian pada parameter *Imperceptibility* menunjukkan bahwa penyisipan *watermark* pada metadata dan *content stream* sama sekali tidak memengaruhi kualitas visual dokumen. Karena kedua penyisipan tersebut berada pada lapisan non-visual dari struktur file PDF.

Penyisipan pada metadata hanya menambahkan informasi deskriptif yang tidak akan ditampilkan pada halaman PDF. Sementara itu, pada penyisipan terhadap *content stream,* watermak akan dibuat sebagai objek baru yang tidak dapat dirender (*non-rendering object*), yang berarti objek tersebut ada dalam struktur file tetapi tidak memiliki instruksi untuk digambar atau ditampilkan secara visual.

Secara kasat mata, tidak ada perbedaan yang signifikan antara dokumen asli dan dokumen yang telah ter-*watermark*, hasil ini membuktikan bahwa *watermark* bersifat tersembunyi dan tidak mengganggu. Hasil ini bisa dilihat pada gambar 3.1.

Hasil Sebelum di watermark

Hasil Setelah di watermark

Gambar 3.1 Perbedaan visual pada dokumen ijazah

3.1.3. *Capacity*

Pengujian dilakukan dengan tujuan untuk mengetahui seberapa besar informasi yang dapat disisipkan kedalam dokumen ijazah digital. Sebanyak 10 sample dokumen ijazah berbeda akan dilakukan untuk pengujian penyisipan watermark. Hasil tersebut disajikan dalam tabel 2 dengan informasi seperti (DW) atau data watermark, (F) atau ukuran asli dokumen, (F') ukuran dokumen setelah dilakukan penyisipan dan (W) menunjukan selisih ukuran antara keduanya dalam bentuk persen. Selisih ukuran W dapat dihasilkan melalui persamaan berikut.

$$W = \frac{F - F'}{F'} \times 100\%$$

Tabel 2. Perubahan Kapasitas pada Dokumen Ijazah Terwatermak.

Sample	F (KB)	DW (KB)	F' (KB)	W %
1	570,41	0,16	571,57	0.20%
2	581,72	0,16	582,86	0.20%
3	582,77	0,16	583,92	0.20%
4	575,52	0,16	576,64	0.19%
5	590,96	0,17	592,09	0.19%
6	578,21	0,16	579,34	0.20%
7	580,16	0,16	581,3	0.20%
8	583,13	0,16	584,26	0.19%
9	585,14	0,16	586,24	0.19%
10	588,69	0,16	589,83	0.19%

Dalam tabel 2 rata-rata perubahan kapasitas sebesar 0.195% ini menunjukkan bahwa penyisipan watermark pada dokumen ijazah digital berhasil dilakukan dan memiliki perubahan yang minim, artinya ukuran file tidak begitu jauh dengan file yang aslinya.

3.2. Deteksi Manipulasi Melalui Analisis Statis

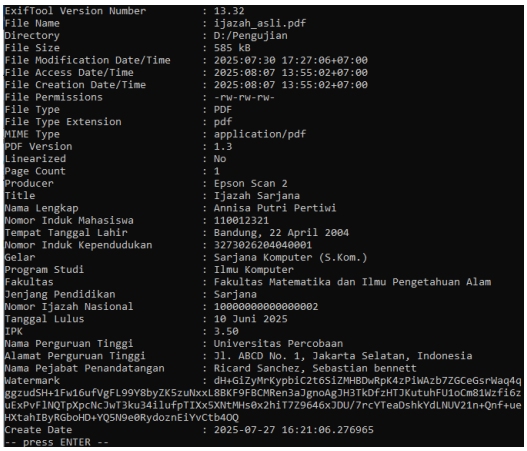
Analisis statis memberikan verifikasi tambahan yang terpisah dari proses *digital watermarking*. Hasilnya dapat menunjukkan kemampuan untuk mendeteksi jejak yang ditinggalkan melalui empat skenario dokumen.

3.2.1 Analisis pada Metadata

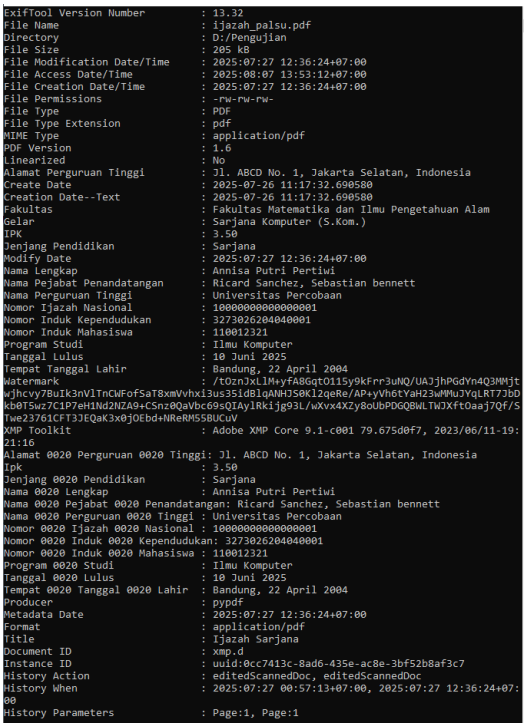
Proses pengambilan nilai metadata akan menggunakan aplikasi *exiftool*, yang nantinya akan mengidentifikasi metadata apa saja yang muncul pada dokumen ijazah tersebut. Sebelum menjelaskan hasil analisis, peneliti akan menidentifikasi metadata apa saja yang akan muncul pada dokumen ijazah yang dibuat, hasil itu meliputi Jenis dokumen, nama lengkap, NIM, tempat tanggal lahir, NIK, dan lain sebagainya. Hal ini bertujuan untuk menetapkan profil metadata standar atau *baseline* untuk dokumen asli. Profil ini kemudian akan digunakan sebagai acuan pembanding untuk mendeteksi setiap perubahan pada dokumen yang akan diverifikasi.

P-ISSN: 2337-8344
E-ISSN: 2623-1247

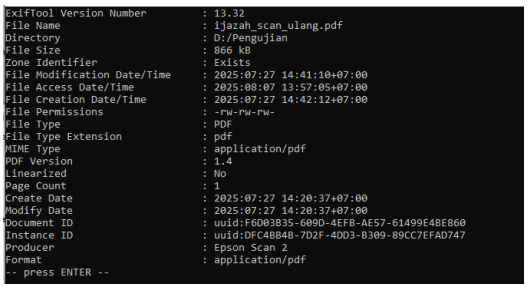
Hasil dari empat skenario dokumen yang dijelaskan sebelumnya akan menampilkan sejumlah metadata yang terdeteksi.



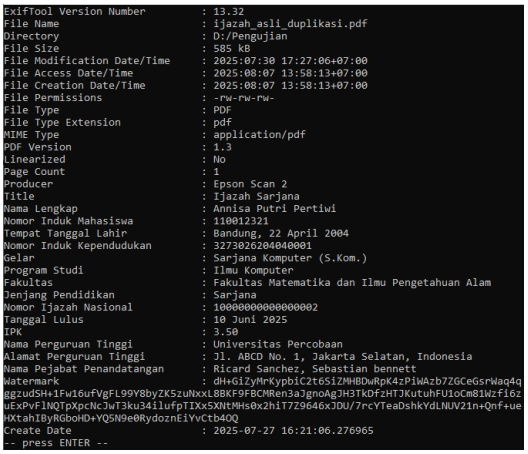
Gambar 3.2 Hasil Ektraksi Metadata Dokumen Ijazah Asli



Gambar 3.3 Hasil Ektraksi Metadata Dokumen Ijazah Modifikasi



Gambar 3.4 Hasil Ektraksi Metadata Dokumen Ijazah Hasil Scan Ulang



Gambar 3.5 Hasil Ektraksi Metadata Dokumen Ijazah Asli yang Diduplikasi

Dokumen yang dimodifikasi meninggalkan jejak yang jelas berupa adanya metadata tambahan seperti XMP Toolkit, yang tidak ada pada dokumen asli. Ini adalah bukti forensik yang kuat bahwa dokumen tersebut telah dibuka dan disimpan ulang oleh aplikasi editor. Selanjutnya, dokumen hasil scan ulang kehilangan hampir semua metadata asli yang ada, termasuk nilai /Watermark yang sudah disisipkan nilai sebelumnya. Kehilangan informasi ini adalah indikator kuat bahwa dokumen tersebut bukan lagi dokumen ijazah digital yang asli.

3.2.2 Analisis pada Struktur PDF

Pada proses analisis ini, penelitian akan menggunakan bantuan library dari python yaitu *pypdf* untuk mengumpulkan bukti struktur dari suatu dokumen ijazah digital. Langkah yang akan dilakukan menggunakan fungsi regex

P-ISSN: 2337-8344
E-ISSN: 2623-1247

untuk mencari nilai objek apa saja yang terdapat dalam dokumen ijazah digital yang sudah terwatermark. Hasil dari pemrograman tersebut akan ditampilkan pada tabel 3.

Tabel 3. Struktur Objek pada Empat Skenario Dokumen

Dokumen Ijazah Asli	Dokumen Ijazah Modifikasi	Dokumen Ijazah Scan Ulang	Dokumen Ijazah Asli yang Diduplikasi
['Pages', 'Catalog', 'Page', 'XObject', 'WatermarkedObject']	['ObjStm', 'ObjStm', 'Catalog', 'Metadata', 'ResourceEvent', 'XObject', 'XObject', 'Font', 'FontDescriptor', 'Font', 'XRef']	['Page', 'XObject', 'Catalog', 'Pages', 'Pages', 'Metadata']	'Pages', 'Catalog', 'Page', 'XObject', 'WatermarkedObject']

Hasil analisis ini mengindikasikan bahwa struktur pada dokumen ijazah dan hasil duplikasinya memiliki urutan yang sama, memiliki objek bernama *WatermarkObject*, yang berarti nilai *watermark* pada proses *embedding* sudah disisipi dalam dokumen tersebut. Pada dokumen modifikasi maupun hasil scan ulang, memiliki struktur yang berbeda, dan hasilnya objek *WatermarkObject* tidak terdapat dalam urutan struktur dokumen.

3.3. Verifikasi pada Protokol Keamanan

Dilakukan sebuah simulasi untuk memverifikasi apakah dokumen yang diberikan asli atau tidak. Simulasi ini menggunakan halaman verifikasi sederhana yang telah dibuat menggunakan library *streamlit* pada python [24], di mana pengguna dapat mengunggah dokumen PDF untuk dianalisis secara otomatis. Halaman ini nantinya akan memberikan hasil akhir berdasarkan dua proses utama yaitu, ekstraksi *digital watermark* dan analisis statis.

Gambar 3.6 Hasil Verifikasi Dokumen Ijazah Asli

Ketika dokumen ijazah asli yang telah diberi *watermark* diunggah ke sistem, proses verifikasi akan berjalan sebagai berikut:

a. **Ekstraksi Watermark:** Sistem berhasil mengekstrak dan mendekripsi *watermark* dari metadata dan *content stream*. Pesan rahasia yang muncul pada kedua penyisipan sesuai dengan data asli mahasiswa.

b. **Analisis Statis:** Sistem Analisis metadata menunjukkan produsen dokumen adalah Epson Scan 2 dan tidak ditemukan jejak modifikasi. Analisis struktur juga menemukan objek /WatermarkedObject yang menjadi bukti bahwa adanya watermark yang sudah disisipkan pada dokumen tersebut.

Maka dari hasil tersebut sistem akan menyatakan bahwa dokumen yang diunggah valid karena dapat menghasilkan pesan rahasia yang sesuai setelah dilakukannya enkripsi, untuk analisis statis, dokumen menunjukan produsen yang sesuai dan struktur yang memiliki objek /WatermarkedObject.

Gambar 3.7 Hasil Verifikasi Dokumen Ijazah Modifikasi

Ketika dokumen ijazah yang sudah dimodifikasi diunggah ke sistem, proses verifikasi akan berjalan sebagai berikut:

a. **Ekstraksi Watermark**: Sistem hanya berhasil mengekstrak dan mendekripsi *watermark* dari salah satu cara penyisipan. Karena disisipkan pada dua cara yaitu pada metadata dan *content* stream, pesan rahasia yang muncul memiliki nilai yang berbeda karena ada salah satu caranya tidak mengeluarkan pesan rahasia.

b. **Analisis Statis**: Sistem Analisis metadata menunjukkan produsen dokumen adalah Epson Scan 2 dan tidak ditemukan jejak modifikasi. Namun analisis struktur tidak menemukan objek /WatermarkedObject.

Dan hasil analisis struktur ini juga menjelaskan bahwa banyaknya objek pada dokumen tersebut sangat jauh beda dengan dokumen asli.

Maka dari hasil tersebut sistem akan menyatakan bahwa dokumen yang diunggah tidak valid atau mencurigakan hal ini berdasarkan hasil dari berbagai faktor seperti ekstraksi watermark yang hanya sebagian dan juga struktur dokumen yang sudah berubah.

Gambar 3.8 Hasil Verifikasi Dokumen Ijazah Hasil Scan

Ketika dokumen ijazah hasil scan ulang diunggah ke sistem, proses verifikasi akan berjalan sebagai berikut:

a. **Ekstraksi Watermark:** Sistem tidak dapat mengekstrak dan mendekripsi *watermark* dari metadata dan *content stream*.

b. **Analisis Statis:** Sistem Analisis metadata menunjukkan produsen dokumen adalah tidak sesuai dengan dokumen. Pada analisis struktur juga tidak menemukan objek /WatermarkedObject.

Maka dari hasil tersebut sistem akan menyatakan bahwa dokumen yang diunggah tidak valid dari berbagai faktor seperti ekstraksi watermark yang tidak ada hasilnya dan juga struktur dokumen yang sudah berubah.

Gambar 3.9 Hasil Verifikasi Dokumen Ijazah Asli yang Diduplikasi

Ketika dokumen ijazah asli yang diduplikasi diunggah ke sistem, proses verifikasi akan berjalan sebagai berikut:

a. **Ekstraksi Watermark:** Sistem berhasil mengekstrak dan mendekripsi *watermark* dari metadata dan *content stream*. Pesan rahasia yang muncul pada kedua penyisipan sesuai dengan data asli mahasiswa.

b. **Analisis Statis:** Sistem Analisis metadata menunjukkan produsen dokumen adalah Epson Scan 2 dan tidak ditemukan jejak modifikasi. Analisis struktur juga menemukan objek /WatermarkedObject yang menjadi bukti bahwa adanya watermark yang sudah disisipkan pada dokumen tersebut.

Maka dari hasil tersebut sistem akan menyatakan bahwa dokumen yang diunggah valid karena dapat menghasilkan pesan rahasia yang sesuai setelah dilakukannya enkripsi, untuk analisis statis, dokumen menunjukan produsen yang sesuai dan struktur yang memiliki objek /WatermarkedObject.

4. KESIMPULAN DAN SARAN

4.1 Kesimpulan

Berdasarkan hasil penelitian yang dilakukan, proses *digital watermark* berhasil melalui tahap pengujian berdasarkan robustness, imperceptibility dan juga capacity dengan perubahan sekitar 0.195% pada hasil dokumen ijazah yang sudah terwatermark. Lalu pada hasil keseluruhan dapat memenuhi kriteria pada sebuah keamanan informasi, hasil tersebut akan menjawab pada aspek kerahasiaan (*Confidentiality*) karena nilai watermark akan disispkan kedalam *content stream* dan metadata dari dokumen ijazah digital, selanjutnya nilai watermark yang terdapat pada dokumen akan berbentuk cipherteks karena sudah dilakukan proses enkripsi menggunakan algoritma AES. Dengan begitu hanya orang yang mempunyai kunci saja yang bisa mendekripsinya. Lalu pada aspek integritas data (*Integrity*) karena setiap perubahan atau modifikasi terhadap dokumen akan mengakibatkan watermark tidak dapat diekstrak secara sempurna. Hal ini membuktikan bahwa protokol keamanan dapat mendeteksi jika dokumen telah mengalami perubahan, baik dari struktur internal maupun metadata-nya. Pada aspek otentifikasi (*Authentication*) berhasil dilakukan karena dengan adanya watermark yang berhasil diekstrak dari dokumen menjadi bukti bahwa dokumen tersebut berasal dari sumber resmi dan belum mengalami pemalsuan. Dengan

demikian, protokol keamanan mampu memenuhi kriteria dalam keamanan informasi.

2.1. Saran

Berdasarkan hasil implementasi dan evaluasi sistem, beberapa saran untuk pengembangan selanjutnya antara lain. Protokol keamanan dapat dikembangkan dengan menambahkan metode watermarking yang terbarukan. Implementasi verifikasi dapat diperluas ke dalam bentuk layanan secara real-time agar lembaga pendidikan melakukan validasi dokumen ijazah digital secara langsung dan terintegrasi dalam sistem informasi akademik.

5. DAFTAR PUSTAKA

[1] A. S. Rosana, "Kemajuan Teknologi Informasi dan Komunikasi dalam Industri Media di Indonesia," *Gema Eksos*, vol. 5, no. 2, 2010.

[2] M. K. Buckland, "What is a 'document'?," *Journal of the American Society for Information Science*, vol. 48, no. 9, pp. 804–809, 1997, doi: 10.1002/(SICI)1097-4571(199709)48:9<804::AID-ASI5>3.0.CO;2-V.

[3] A. Castiglione, A. De Santis, and C. Soriente, "Security and privacy issues in the Portable Document Format," *Journal of Systems and Software*, vol. 83, no. 10, 2010, doi: 10.1016/j.jss.2010.04.062.

[4] W. Setiawan, "Era Digital dan Tantangannya," *Seminar Nasional Pendidikan* , 2017.

[5] Q. Abu Al-Haija, A. Odeh, and H. Qattous, "PDF Malware Detection Based on Optimizable Decision Trees," *Electronics (Switzerland)*, vol. 11, no. 19, 2022, doi: 10.3390/electronics11193142.

[6] P. S. Ramadhan, M. Syahril, R. Kustini, H. Winata, and R. D. Gea, "Transaction Data Security Using AES and RC4," *CESS (Journal of Computer Engineering, System and Science)*, vol. 8, no. 1, 2023, doi: 10.24114/cess.v8i1.41212.

[7] M. Sreerama Murty, D. Veeraiah, and A. Srinivas Rao, "Digital Signature and Watermark Methods For Image Authentication using Cryptography Analysis," *Signal Image Process*, vol. 2, no. 2, pp. 170–179, Jun. 2011, doi: 10.5121/sipij.2011.2214.

[8] B. LeBeau, "pdfsearch: Search Tools for PDF Files," *J Open Source Softw*, vol. 3, no. 27, 2018, doi: 10.21105/joss.00668.

[9] J. P. Donaldson and G. W. Dinolt, "SOURCE FINGERPRINTING IN ADOBE PDF FILES," 2013.

[10] C. T. Hsu and J. L. Wu, "Hidden digital watermarks in images," *IEEE Transactions on Image Processing*, vol. 8, no. 1, 1999, doi: 10.1109/83.736686.

[11] A. Suheryadi, "PENERAPAN DIGITAL WATERMARK SEBAGAI VALIDASI KEABSAHAN GAMBAR DIGITAL DENGAN SKEMA BLIND WATERMARK," *JTT (Jurnal Teknologi Terapan)*, vol. 3, no. 2, 2017, doi: 10.31884/jtt.v3i2.54.

[12] A. R. Pambudi, Garno, and Purwantoro, "DETEKSI KEASLIAN UANG KERTAS BERDASARKAN WATERMARK DENGAN PENGOLAHAN CITRA DIGITAL," *Jurnal Informatika Polinema*, vol. 6, no. 4, 2020, doi: 10.33795/jip.v6i4.407.

[13] A. Apriliani, K. Hijjayanti, and S. Suhairoh, "Analisis Keaslian Citra Dengan Menggunakan Exif Metadata," *CESS (Journal of Computer Engineering, System and Science)*, vol. 5, no. 1, p. 84, Jan. 2020, doi: 10.24114/cess.v5i1.15600.

[14] K. Eka Purnama, C. Rozikin, and A. Ali Ridha, "ANALISIS FORENSIC CITRA DIGITAL MENGGUNAKAN TEKNIK ERROR LEVEL ANALYSIS DAN METADATA BERDASARKAN METODE NIST," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 7, no. 2, pp. 1100–1107, Aug. 2023, doi: 10.36040/jati.v7i2.6660.

[15] S. H. Supangkat, Kuspriyanto, and Juanda, "Watermarking sebagai Teknik Penyembunyian Label Hak Cipta pada Data Digital," 2000.

[16] M. Arnold, M. Schmucker, and Stephen D. Wolthusen, *Techniques and Applications of Digital Watermarking and Content Protection*. 2003. [Online]. Available: http://www.esecurity.ch/serieseditor.html

[17] A. Nugrahantoro, A. Fadlil, and I. Riadi, "Optimasi Keamanan Informasi Menggunakan Algoritma Advanced Encryption Standard (AES) Mode Chiper Block Chaining (CBC)," *Jurnal Ilmiah FIFO*, vol. 12, no. 1, p. 12, Jul. 2020, doi: 10.22441/fifo.2020.v12i1.002.

[18] A. Systems Incorporated, "PDF Reference fifth edition Adobe® Portable Document Format Adobe Systems Incorporated," 1985.

[19] M. Rafique and M. N. A. Khan, "Exploring Static and Live Digital Forensics: Methods, Practices and Tools," *Int J Sci Eng Res*, vol. 4, no. 10, pp. 1048–1056, 2013, [Online]. Available: http://www.ijser.org/researchpaper%5CExploring-Static-and-Live-Digital-Forensic-Methods-Practices-and-Tools.pdf

[20] A. I. Putra, R. Umar, and A. Fadlil, "Analisis Forensik Deteksi Keaslian Metadata Video Menggunakan Exiftool," *Seminar Nasional Informatika 2018 (semnasIF 2018) UPN Yogyakarta*, vol. 2018, 2018.

[21] W. Zhao, H. Guan, and S. Zhang, "Research and Implementation of Text Watermarking Technology Based on PDF Document Structure," *International Journal of Frontiers in Sociology*, vol. 2, pp. 1–9, doi: 10.25236/IJFS.2020.020101.

[22] Adobe, "Adobe Acrobat User Guide." Accessed: Jul. 31, 2025. [Online]. Available: https://helpx.adobe.com/acrobat/user-guide.html

[23] R. J. B. B. Amirtharajan R., "Inverted pattern in inverted time domain for icon steganography," *Information Technology Journal*, vol. 11, pp. 587–595, 2012.

[24] Snowflake Inc., "Streamlit Documentation." Accessed: Jul. 31, 2025. [Online]. Available: https://docs.streamlit.io/