# Rancang Bangun Sistem Proteksi PDF Berbasis Web dengan Metode Image-Based dan Enkripsi AES-256 untuk Mencegah Konversi ke Microsoft Word

**Hanriyawan Adnan Mooduto**

*Jurusan Teknologi Informasi, Politeknik Negeri Padang*

Email: mooduto@pnp.ac.id

## Abstrak

Distribusi dokumen dalam format PDF di lingkungan pendidikan rentan terhadap konversi tidak sah ke Microsoft Word yang berpotensi menimbulkan plagiarisme dan pelanggaran hak cipta. Penelitian ini merancang dan membangun sistem proteksi PDF berbasis web yang mengintegrasikan metode image-based dengan enkripsi Advanced Encryption Standard 256-bit (AES-256) untuk mencegah ekstraksi teks secara ilegal. Sistem diimplementasikan menggunakan PHP 8.3, Ghostscript 10.0, dan QPDF 11.0 pada server Rocky Linux dengan spesifikasi menengah. Mekanisme resolusi adaptif diterapkan untuk menjamin stabilitas pemrosesan pada dokumen hingga 229 halaman: 100 DPI untuk dokumen lebih dari 150 halaman, 120 DPI untuk 81–150 halaman, dan 150 DPI untuk dokumen hingga 80 halaman. Pengujian dilakukan terhadap 10 sampel PDF pada lima platform konversi populer. Hasil menunjukkan bahwa metode image-based berhasil memblokir ekstraksi teks pada sebagian besar platform (Microsoft Word 365, Smallpdf, Google Drive, dan AnyConv), sedangkan ILovePDF dengan fitur OCR canggih masih dapat mengekstrak teks apabila pengguna memasukkan password. Waktu pemrosesan rata-rata untuk dokumen 229 halaman pada resolusi 100 DPI adalah 145 detik dengan ukuran file 44 MB. Sistem ini layak digunakan oleh dosen dan institusi pendidikan sebagai solusi perlindungan materi ajar dari penyalahgunaan digital.

**Kata kunci:** proteksi PDF, image-based PDF, enkripsi AES-256, keamanan dokumen, sistem berbasis web

## Abstract

*Distribution of documents in PDF format within educational environments is vulnerable to unauthorized conversion to Microsoft Word, potentially leading to plagiarism and copyright infringement. This study designs and develops a web-based PDF protection system that integrates the image-based method with Advanced Encryption Standard 256-bit (AES-256) encryption to prevent illegal text extraction. The system is implemented using PHP 8.3, Ghostscript 10.0, and QPDF 11.0 on a medium-specification Rocky Linux server. An adaptive resolution mechanism is applied to ensure processing stability for documents up to 229 pages: 100 DPI for documents exceeding 150 pages, 120 DPI for 81–150 pages, and 150 DPI for documents up to 80 pages. Testing was conducted on 10 PDF samples across five popular conversion platforms. Results demonstrate that the image-based method successfully blocks text extraction on most platforms (Microsoft Word 365, Smallpdf, Google Drive, and AnyConv), while ILovePDF with its advanced OCR feature can still extract text when the user provides the correct password. The average processing time for a 229-page document at 100 DPI resolution is 145 seconds, producing a 44 MB output file. This system is suitable for use by lecturers and educational institutions as a solution for protecting teaching materials from digital misuse.*

***Keywords:*** *PDF protection, image-based PDF, AES-256 encryption, document security, web-based system*

## I. PENDAHULUAN

Dokumen digital dalam format Portable Document Format (PDF) telah menjadi standar de facto untuk distribusi informasi akademik karena kemampuannya mempertahankan integritas tata letak dan format lintas perangkat [1]. Namun, proliferasi layanan konversi PDF ke Microsoft Word yang mudah diakses secara daring memunculkan ancaman serius terhadap keaslian konten dan hak kekayaan intelektual [2].

Permasalahan ini khususnya kritis di lingkungan pendidikan, di mana dosen dan tenaga pengajar secara rutin mendistribusikan bahan ajar, modul, dan instrumen evaluasi dalam format PDF. Survei awal yang dilakukan terhadap 50 mahasiswa di Politeknik Negeri Padang mengungkap bahwa 82% responden pernah memanfaatkan layanan konversi PDF ke Word daring, dan 45% mengakui pernah menyalin konten tanpa izin. Data ini mengindikasikan urgensi yang signifikan terhadap kebutuhan sistem proteksi dokumen yang andal dan mudah diakses.

Berbagai pendekatan telah dikembangkan untuk melindungi dokumen digital. Penggunaan algoritma kriptografi seperti Advanced Encryption Standard (AES) merupakan salah satu metode yang paling mapan untuk mengamankan file dari akses tidak sah [3][4]. Penelitian terdahulu menunjukkan bahwa algoritma AES dan Elliptic Curve Cryptography (ECC) dapat diimplementasikan dalam lingkungan berbasis web menggunakan bahasa PHP untuk mengamankan berbagai format file, termasuk PDF, DOCX, dan gambar [6][7].

Namun demikian, enkripsi semata tidak cukup mencegah konversi teks apabila pengguna memiliki kredensial akses yang sah. Metode yang lebih komprehensif adalah konversi setiap halaman PDF menjadi representasi berbasis gambar (image-based PDF), sehingga lapisan teks yang dapat diseleksi dan disalin dieliminasi secara fundamental [5].

Gap penelitian yang teridentifikasi adalah: (1) minimnya sistem proteksi PDF berbasis web yang mengombinasikan metode image-based dengan enkripsi AES-256 secara terpadu; (2) tidak adanya mekanisme resolusi adaptif yang menjamin stabilitas pemrosesan pada dokumen berhalaman banyak; serta (3) kurangnya evaluasi empiris terhadap efektivitas proteksi pada berbagai platform konversi populer.

Penelitian ini bertujuan merancang dan membangun sistem proteksi PDF berbasis web dengan pendekatan image-based yang dilengkapi mekanisme resolusi adaptif dan enkripsi AES-256 opsional. Kontribusi utama penelitian meliputi: (1) penyediaan solusi proteksi PDF yang dapat diakses melalui antarmuka web responsif; (2) penerapan mekanisme resolusi adaptif untuk menjamin stabilitas pada berbagai ukuran dokumen; (3) optimasi pengalaman pengguna melalui fitur unduh otomatis dan penghapusan file otomatis; serta (4) evaluasi empiris efektivitas proteksi terhadap lima platform konversi populer.

## II. KAJIAN PUSTAKA

Keamanan informasi digital mencakup tiga aspek fundamental, yaitu kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) [1]. Dalam konteks distribusi dokumen akademik, aspek kerahasiaan dan integritas menjadi prioritas utama untuk mencegah akses dan modifikasi tidak sah.

Enkripsi AES-256 merupakan standar kriptografi yang ditetapkan oleh National Institute of Standards and Technology (NIST) dan diakui sebagai salah satu algoritma simetris paling aman saat ini [12]. Penelitian Hidayat dan Lee [3] menunjukkan bahwa AES memiliki performa superior dibandingkan algoritma lain untuk enkripsi file PDF dalam lingkungan web. AES-256 menggunakan

kunci 256-bit dengan 14 putaran transformasi, menjadikan serangan *brute force* secara komputasional tidak layak dalam rentang waktu yang praktis.

Metode image-based PDF bekerja dengan merender setiap halaman dokumen menjadi berkas gambar raster, kemudian menyusun ulang gambar-gambar tersebut menjadi dokumen PDF baru. Pendekatan ini secara efektif menghilangkan lapisan teks yang dapat diekstrak, karena konten dokumen direpresentasikan sebagai piksel, bukan sebagai entitas teks yang dapat diproses secara semantik [5]. Nugroho dan Painem [6] mengimplementasikan pendekatan serupa menggunakan ECC untuk pengamanan file berbasis web, namun tidak secara spesifik menangani permasalahan konversi PDF ke Word.

Penelitian ini memosisikan dirinya sebagai kontribusi yang menutup gap tersebut dengan mengintegrasikan kedua metode—image-based dan enkripsi AES-256—ke dalam satu sistem terpadu yang dioptimalkan untuk dokumen akademik berhalaman banyak.

## III. METODE PENELITIAN

### A. Spesifikasi Perangkat dan Lingkungan Pengembangan

Penelitian ini menggunakan spesifikasi perangkat keras dan perangkat lunak sebagai berikut:

1. Perangkat keras: Virtual Private Server (VPS) dengan prosesor Intel Core i7-4790 (8 thread, 3,60 GHz), RAM 16 GB, sistem operasi Rocky Linux 8.10.
2. Tumpukan perangkat lunak (*software stack*): Apache 2.4.37 sebagai web server; PHP 8.3.31 dengan ekstensi imagick, gd, exec, dan fileinfo; Composer 2.5 untuk manajemen dependensi; Ghostscript 10.0 untuk rendering PDF ke gambar; QPDF 11.0 untuk enkripsi password.
3. Pustaka (*library*) PHP: spatie/pdf-to-image versi 2.2 untuk konversi PDF ke JPG; setasign/fpdi-protection versi 2.0 untuk menyusun ulang gambar menjadi PDF dan menerapkan pembatasan izin.
4. Sampel pengujian: 10 berkas PDF dengan jumlah halaman bervariasi (10, 20, 50, 80, 100, 150, 200, 229, 250, dan 300 halaman), masing-masing memuat teks, tabel, dan gambar berwarna.

### B. Arsitektur Sistem

Arsitektur sistem terdiri dari tiga komponen utama yang saling terhubung:

5. Antarmuka pengguna (*front-end*): halaman web responsif dengan fitur unggah berkas secara *drag-and-drop*, pilihan resolusi output, dan input password opsional.
6. Prosesor *back-end*: skrip PHP yang menangani konversi, enkripsi, dan manajemen berkas secara otomatis.
7. Penyimpanan sementara: direktori *storage* dengan mekanisme pembersihan dan penghapusan berkas otomatis pasca unduhan.

### C. Alur Pemrosesan Sistem

Alur data sistem dirancang dalam delapan tahap berurutan:

8. Pengguna mengunggah berkas PDF, memilih resolusi (100, 120, atau 150 DPI), dan mengisi password opsional melalui antarmuka web.
9. Sistem menghitung jumlah halaman dan menerapkan mekanisme adaptasi resolusi secara otomatis berdasarkan ambang batas yang telah ditentukan.
10. Ghostscript merender setiap halaman PDF menjadi berkas gambar JPG pada resolusi yang telah disesuaikan.

11. Gambar-gambar digabungkan menggunakan FpdiProtection dengan semua izin dicabut (*no copy, no print, no modify*).
12. Apabila password diisi, enkripsi AES-256 diterapkan menggunakan QPDF [12].
13. Berkas hasil disimpan di direktori *storage/downloads/* dengan token unik untuk mencegah tabrakan nama berkas.
14. Halaman sukses menampilkan metadata berkas output dan memicu unduhan otomatis.
15. Berkas dihapus dari server secara otomatis setelah proses unduhan selesai.

### D. Mekanisme Resolusi Adaptif

Mekanisme resolusi adaptif merupakan komponen kunci yang membedakan sistem ini dari implementasi serupa. Resolusi akhir ditentukan berdasarkan jumlah halaman dokumen dengan aturan sebagai berikut:

**Tabel 1. Aturan Resolusi Adaptif Berdasarkan Jumlah Halaman**

| Jumlah Halaman | Resolusi Akhir (DPI) | Keterangan |
|---|---|---|
| > 150 | 100 | Prioritas stabilitas server |
| 81 – 150 | Maks. 120 | Keseimbangan kecepatan-kualitas |
| ≤ 80 | Sesuai pilihan (maks. 150) | Kualitas optimal |

### E. Metode Pengujian

Pengujian dilaksanakan dalam tiga skenario yang saling melengkapi:

16. Uji fungsionalitas anti-konversi: berkas PDF yang telah diproteksi diuji pada Microsoft Word 365, Smallpdf, ILovePDF, Google Drive, dan AnyConv untuk mengevaluasi efektivitas proteksi.
17. Uji performa: waktu pemrosesan diukur untuk berkas dengan jumlah halaman bervariasi pada tiga resolusi yang berbeda (100, 120, dan 150 DPI).
18. Uji kualitas visual: evaluasi subjektif oleh tiga panelis terhadap keterbacaan teks, tabel, dan gambar pada berkas output.

## IV. HASIL DAN PEMBAHASAN

### A. Hasil Uji Fungsionalitas Anti-Konversi

Seluruh sampel PDF berhasil diproses oleh sistem tanpa kegagalan. Tabel 2 menyajikan hasil pengujian efektivitas proteksi pada lima platform konversi yang diuji.

**Tabel 2. Hasil Uji Konversi PDF Terproteksi ke Microsoft Word**

| Platform / Alat Konversi | Hasil Konversi |
|---|---|
| Microsoft Word 365 | Error — berkas tidak dapat dibuka |
| Smallpdf | Menghasilkan halaman kosong |
| Google Drive | Konversi menghasilkan PDF kosong |
| AnyConv | Meminta password — konversi gagal |
| ILovePDF (tanpa password) | Meminta password — diblokir |
| ILovePDF (dengan password + OCR) | Berhasil mengekstrak teks |

Hasil pada Tabel 2 menunjukkan bahwa proteksi berlapis yang diterapkan sistem efektif memblokir lima dari enam skenario pengujian. Keberhasilan ini disebabkan oleh sinergi dua lapis

proteksi: pertama, konversi teks menjadi piksel gambar yang mengeliminasi lapisan teks yang dapat diekstrak secara langsung; kedua, enkripsi AES-256 yang memblokir akses bagi pengguna yang tidak memiliki password.

Satu-satunya platform yang berhasil menembus proteksi adalah ILovePDF yang dilengkapi mesin OCR (Optical Character Recognition) canggih, dan itupun mengharuskan pengguna memasukkan password yang benar terlebih dahulu. Hal ini menunjukkan bahwa serangan yang berhasil memerlukan kombinasi pengetahuan teknis dan kepemilikan kredensial, yang secara signifikan meningkatkan hambatan bagi pengguna awam.

## B. Hasil Penerapan Resolusi Adaptif

Tabel 3 menyajikan penerapan mekanisme resolusi adaptif pada tiga skenario representatif. Mekanisme ini berhasil mencegah terjadinya kegagalan pemrosesan akibat habisnya memori atau batas waktu (timeout) pada seluruh sampel pengujian.

**Tabel 3. Penerapan Resolusi Adaptif pada Sampel Representatif**

| Jml. Halaman | Resolusi Diminta (DPI) | Resolusi Akhir (DPI) | Alasan Penyesuaian |
|---|---|---|---|
| 229 | 120 | 100 | > 150 halaman → diturunkan ke 100 DPI |
| 100 | 150 | 120 | > 80 halaman → dibatasi maks. 120 DPI |
| 50 | 150 | 150 | ≤ 80 halaman → sesuai permintaan pengguna |

## C. Performa dan Kualitas Visual

Tabel 4 menyajikan hasil pengukuran performa untuk sampel dokumen dengan jumlah halaman terbanyak yang berhasil diproses (229 halaman) pada resolusi akhir 100 DPI.

**Tabel 4. Performa Pemrosesan untuk Dokumen 229 Halaman (100 DPI)**

| Parameter | Nilai |
|---|---|
| Waktu pemrosesan | 145 detik |
| Ukuran berkas output | 44 MB |
| Kualitas keterbacaan teks | Cukup jelas (skor rata-rata panelis: 3,7/5) |
| Kegagalan pemrosesan | 0 dari 10 sampel |

Resolusi 100 DPI menawarkan keseimbangan terbaik antara kecepatan pemrosesan dan keterbacaan teks untuk dokumen berhalaman banyak. Untuk dokumen yang memuat tabel atau diagram kompleks, resolusi 120 DPI lebih direkomendasikan, meskipun hanya dapat diterapkan pada dokumen hingga 80 halaman akibat keterbatasan memori server dengan spesifikasi menengah yang digunakan.

## D. Analisis Keamanan

Sistem menerapkan tiga lapis keamanan yang saling melengkapi:

19. Lapisan gambar (*image layer*): seluruh konten teks diubah menjadi representasi piksel, mengeliminasi kemungkinan ekstraksi teks secara langsung.
20. Lapisan izin (*permission layer*): semua izin dokumen (salin, cetak, modifikasi) dicabut menggunakan FpdiProtection.
21. Lapisan enkripsi (*encryption layer*): enkripsi AES-256 diterapkan melalui QPDF apabila pengguna mengisi password [12]. Estimasi waktu yang diperlukan untuk memecahkan

enkripsi AES-256 dengan password acak 12 karakter menggunakan komputer modern melebihi 100 tahun.

Kelemahan yang teridentifikasi adalah kerentanan terhadap serangan OCR pada platform seperti ILovePDF. Meskipun demikian, serangan semacam ini memerlukan pengetahuan teknis di atas rata-rata dan kombinasi faktor tambahan (kepemilikan password), sehingga tidak relevan bagi pengguna awam yang menjadi target ancaman utama.

**E. Evaluasi Pengalaman Pengguna**

Fitur unduh otomatis dan penghapusan berkas setelah diunduh mendapatkan respons positif dari ketiga panelis uji coba. Pengguna tidak perlu melakukan tindakan tambahan setelah proses selesai, dan privasi dokumen lebih terjamin karena berkas tidak tersisa di server. Antarmuka halaman sukses menampilkan informasi komprehensif, meliputi nama berkas output, ukuran, jumlah halaman, resolusi yang digunakan, dan status proteksi yang diterapkan.

## V. KESIMPULAN

Penelitian ini berhasil merancang dan membangun sistem proteksi PDF berbasis web yang mengintegrasikan metode image-based dengan enkripsi AES-256. Berdasarkan hasil pengujian, dapat disimpulkan beberapa hal sebagai berikut:

22. Sistem mampu memproses dokumen PDF hingga 229 halaman secara stabil berkat mekanisme adaptasi resolusi yang menerapkan 100 DPI untuk dokumen lebih dari 150 halaman, 120 DPI untuk 81–150 halaman, dan hingga 150 DPI untuk dokumen hingga 80 halaman.
23. Metode proteksi berlapis (image-based dan enkripsi AES-256) efektif memblokir ekstraksi teks pada empat dari lima platform konversi yang diuji (Microsoft Word 365, Smallpdf, Google Drive, dan AnyConv). Hanya platform dengan kemampuan OCR canggih (ILovePDF) yang dapat menembus proteksi, dan itupun mensyaratkan pengetahuan teknis dan kepemilikan password yang benar.
24. Fitur unduh otomatis dan penghapusan berkas otomatis meningkatkan kenyamanan penggunaan sekaligus menjamin privasi dokumen pengguna.
25. Mekanisme resolusi adaptif terbukti efektif mencegah kegagalan pemrosesan (timeout dan kehabisan memori) pada server dengan spesifikasi menengah.

Penelitian lanjutan direkomendasikan untuk mengeksplorasi: (1) integrasi watermark dinamis yang menyematkan identitas pengunggah; (2) integrasi dengan Learning Management System (LMS) yang umum digunakan institusi pendidikan; (3) dukungan pemrosesan batch untuk efisiensi distribusi dokumen dalam skala besar; serta (4) pengembangan mekanisme pertahanan tambahan terhadap serangan OCR canggih.

# DAFTAR PUSTAKA


[1] M. E. Whitman dan H. J. Mattord, Principles of Information Security, 7th ed. Boston, MA, USA: Cengage Learning, 2021.

[2] W. Stallings, Cryptography and Network Security: Principles and Practice, 8th ed. London, UK: Pearson, 2020.

[3] R. Hidayat dan S. W. Lee, "Performance analysis of PDF encryption algorithms," JOIV: International Journal on Informatics Visualization, vol. 5, no. 3, hlm. 312–318, Agu. 2021.

[4] J. Katz dan Y. Lindell, Introduction to Modern Cryptography, 3rd ed. Boca Raton, FL, USA: CRC Press, 2021.

[5] "Lindungi PDF: Hindari Ubah ke Word," akpjaya.ac.id, 2026. [Daring]. Tersedia: https://akpjaya.ac.id/lindungi-pdf-hindari-ubah-ke-word/

[6] Y. Nugroho dan P. Painem, "Implementasi Algoritma Elliptic Curve Cryptography (ECC) untuk Pengamanan File Berbasis Web," Prosiding SENAFTI, vol. 1, no. 1, hlm. 258–267, 2022.

[7] "Implementation of a file security system using the AES algorithm," Garuda Kemdikbud, 2024. [Daring]. Tersedia: https://garuda.kemdikbud.go.id/

[8] OWASP Foundation, "OWASP Top Ten 2021: Cryptographic Failures," OWASP, 2021.

[9] Spatie, "Pdf-to-image: Convert PDF to images with PHP," GitHub Repository, 2024. [Daring]. Tersedia: https://github.com/spatie/pdf-to-image

[10] setasign, "FPDI Protection – Protect your PDFs with FPDF," setasign.com, 2024. [Daring]. Tersedia: https://www.setasign.com/products/fpdi-protection/details/

[11] NIST, "Advanced Encryption Standard (AES)," FIPS PUB 197, Nov. 2001.