Kompresi Citra Dokumen Rahasia Menggunakan Bit-Plane Slicing dan Huffman Coding dengan Selective Encryption

Muhammad Fauzan Azhim
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
mfauzan.az23@gmail.com

***Ringkasan*—Keamanan dan efisiensi penyimpanan merupakan dua aspek krusial dalam pengelolaan citra dokumen rahasia seperti dokumen pemerintahan, medis, dan hukum. Penelitian ini mengimplementasikan dan mengevaluasi metode kompresi citra digital yang menggabungkan teknik *bit-plane slicing* dan *Huffman coding* dengan *selective encryption* pada bit-plane yang paling signifikan. Bit-plane slicing memecah citra grayscale 8-bit menjadi 8 layer bit biner, di mana empat bit paling signifikan (MSB: P7-P4) mengandung sekitar 99% informasi visual. Selective encryption diterapkan menggunakan operasi XOR dengan *keystream* pseudorandom hanya pada keempat MSB tersebut, sementara empat bit paling rendah (LSB: P3-P0) tetap tidak terenkripsi untuk memaksimalkan efisiensi kompresi. Setiap bit-plane kemudian dikompresi menggunakan Run-Length Encoding (RLE) diikuti Huffman coding. Hasil eksperimen pada 2 citra dokumen menunjukkan bahwa metode ini memberikan overhead enkripsi rata-rata sebesar 79,36%, sambil mempertahankan rekonstruksi *lossless* sempurna (PSNR = ∞, SSIM = 1.0) dan keamanan visual yang kuat. Tanpa kunci dekripsi yang benar, citra hasil dekompresi menampilkan distorsi berat sehingga informasi asli tidak dapat dikenali. Metode ini efektif untuk aplikasi yang membutuhkan keseimbangan antara kompresi efisien dan keamanan data.**

***Index Terms*—kompresi citra, bit-plane slicing, Huffman coding, selective encryption, keamanan dokumen**

I. Pendahuluan

A. Latar Belakang

Dokumen-dokumen penting seperti surat keputusan pemerintah, rekam medis pasien, atau berkas legal sering kali dipindai dan disimpan dalam bentuk citra digital. Citra dokumen tersebut biasanya disimpan atau ditransmisikan dalam format gambar populer seperti PNG (lossless) atau JPEG (lossy). Dalam pengelolaan dokumen digital, dua tantangan utama yang dihadapi adalah: (1) bagaimana mengompresi citra agar berukuran kecil untuk efisiensi penyimpanan dan transmisi, dan (2) bagaimana menjaga kerahasiaan informasi sensitif yang terkandung dalam dokumen tersebut.

Secara tradisional, pendekatan yang umum digunakan adalah mengenkripsi seluruh berkas setelah proses kompresi (*compress-then-encrypt*). Meskipun efektif dari segi keamanan, pendekatan ini memiliki beberapa kelemahan: overhead komputasi yang signifikan karena seluruh data harus diacak, kurangnya fleksibilitas karena penerima harus mendekripsi seluruh berkas untuk melihat isinya, dan ketidaksesuaian dengan beberapa aplikasi yang membutuhkan akses sebagian data.

B. Selective Encryption sebagai Solusi

Untuk mengatasi keterbatasan enkripsi penuh, pendekatan *selective encryption* (enkripsi selektif) muncul sebagai solusi yang lebih efisien. Alih-alih mengenkripsi seluruh berkas, selective encryption hanya mengenkripsi sebagian data yang paling sensitif atau signifikan secara visual. Dalam konteks citra digital, bit-bit yang sangat menentukan tampilan gambar dienkripsi, sedangkan sisanya dibiarkan dalam bentuk terkompresi biasa. Dengan demikian, ukuran berkas dan kompatibilitas format dapat tetap terjaga, overhead enkripsi berkurang, namun isi dokumen tetap tersamar bagi pihak yang tidak memiliki kunci dekripsi.

C. Bit-Plane Slicing dan Selective Encryption

Penelitian ini mengusulkan pendekatan yang menggabungkan *bit-plane slicing*, *Huffman coding*, dan *selective encryption* untuk kompresi citra dokumen rahasia. Inti gagasannya adalah bahwa bit-plane yang paling signifikan (MSB) dari citra mengandung sebagian besar informasi visual penting. Dengan mengenkripsi hanya lapisan bit MSB (P7, P6, P5, P4), citra hasil kompresi akan menjadi tidak dapat dibaca isinya tanpa kunci yang tepat, sementara bit-plane LSB (P3, P2, P1, P0) tetap dapat dikompresi secara optimal.

D. Tujuan Penelitian

Tujuan dari penelitian ini adalah:

- Mengimplementasikan sistem kompresi citra dokumen menggunakan bit-plane slicing dan Huffman coding dengan selective encryption.
- Mengevaluasi kinerja kompresi dari segi rasio kompresi, waktu pemrosesan, dan overhead enkripsi.
- Memverifikasi bahwa rekonstruksi citra bersifat *lossless* (tanpa kehilangan informasi).
- Menganalisis keefektifan enkripsi selektif dalam menyembunyikan informasi visual.

E. Kontribusi

Kontribusi utama penelitian ini meliputi:

- Implementasi lengkap sistem kompresi dengan selective encryption dalam bahasa Python dengan dokumentasi komprehensif.
- Evaluasi eksperimental pada citra dokumen nyata dengan pengukuran metrik kompresi, keamanan, dan kinerja.
- Analisis trade-off antara efisiensi kompresi dan keamanan enkripsi pada pendekatan selective encryption.

II. Tinjauan Pustaka

A. Bit-Plane Slicing

Bit-plane slicing adalah teknik dalam pemrosesan citra yang memisahkan citra grayscale 8-bit menjadi delapan citra biner (bit-plane) terpisah, masing-masing merepresentasikan satu bit pada posisi tertentu dalam representasi biner setiap piksel [1]. Secara matematis, bit-plane ke-i dari citra $I(x, y)$ dapat diperoleh dengan:

$$P_i(x, y) = \left\lfloor \frac{I(x, y)}{2^i} \right\rfloor \bmod 2 \tag{1}$$

di mana $i = 0, 1, ..., 7$ untuk citra 8-bit. Bit-plane paling signifikan (P7 atau bit ke-7) mengandung pola objek yang paling mirip dengan citra asli, sementara bit-plane paling rendah (P0) umumnya berisi noise atau detail halus yang kontribusinya minimal terhadap tampilan citra.

Keuntungan bit-plane slicing adalah kemampuannya mengidentifikasi komponen penting dan kurang penting dari citra. Bit-plane MSB cenderung memiliki pola berkorelasi dan area konstan yang dapat dikompresi secara efisien menggunakan teknik seperti Run-Length Encoding (RLE).

B. Huffman Coding

Huffman coding merupakan algoritma pengkodean entropi yang memanfaatkan frekuensi kemunculan simbol untuk menghasilkan kode biner dengan panjang bit variabel [2]. Simbol yang lebih sering muncul diberi kode lebih pendek, sehingga keseluruhan ukuran data terkompresi menjadi lebih kecil. Algoritma Huffman banyak digunakan dalam format kompresi standar seperti JPEG dan PNG.

Dalam konteks penelitian ini, Huffman coding digunakan untuk mengompresi bit-bit hasil bit-plane slicing. Dengan mengombinasikan Huffman coding dan RLE pada tiap bit-plane, pola bit berulang dapat diwakili dengan kode yang sangat singkat.

C. Selective Encryption

Selective encryption adalah teknik enkripsi di mana hanya sebagian data yang dianggap penting atau sensitif yang dienkripsi, sementara sisanya dibiarkan dalam bentuk asli atau terkompresi [5]. Van Droogenbroeck dan Benedett (2002) merumuskan beberapa persyaratan selective encryption pada citra terkompresi: (a) secara visual, hasil enkripsi sebagian harus cukup mengacak citra sehingga informasi penting tidak terlihat, (b) enkripsi dilakukan setelah tahap kompresi dan hanya pada bagian bitstream tertentu, (c) ukuran bitstream tidak berubah signifikan, dan (d) bitstream terenkripsi tetap sesuai format sehingga dapat dibuka dengan decoder standar.

Munir (2012) menunjukkan bahwa bit-bit MSB suatu citra grayscale menentukan rupa objek di citra tersebut, sementara bit-bit LSB tampak acak [3]. Penelitian tersebut menemukan bahwa mengenskripsi 4 bit MSB (P7-P4) adalah pilihan optimal antara keamanan dan kinerja: hanya sekitar 50% data yang dienkripsi, namun citra hasil akhirnya sudah sangat teracak dan keamanan tetap terjamin.

D. Penelitian Terkait

Radhakrishnan dkk. (2012) melaporkan algoritma kompresi HALIC berbasis bit-plane slicing dan Huffman yang mampu mengalahkan standar JPEG-LS dan CALIC dalam efisiensi kompresi pada citra medis dan satelit [4]. Ini mengindikasikan bahwa bit-plane slicing adalah pendekatan menjanjikan untuk kompresi lossless pada citra berstruktur tertentu seperti dokumen.

III. Metodologi

A. Arsitektur Sistem

Sistem yang diusulkan terdiri dari pipeline kompresi dan dekompresi yang terintegrasi. Pipeline kompresi meliputi: (1) dekomposisi bit-plane, (2) selective encryption pada MSB, (3) RLE encoding, dan (4) Huffman coding. Pipeline dekompresi merupakan kebalikan dari proses tersebut.

B. Dekomposisi Bit-Plane

Citra dokumen input (grayscale 8-bit) diuraikan menjadi delapan bit-plane biner terpisah menggunakan operasi bitwise. Untuk setiap piksel dengan nilai intensitas $I(x, y)$, bit ke-i diekstrak menggunakan:

$$P_i(x, y) = (I(x, y) \gg i) \wedge 1 \tag{2}$$

di mana $\gg$ adalah operasi *right shift* dan $\wedge$ adalah operasi bitwise AND. Proses ini menghasilkan 8 layer citra biner: $P_0, P_1, ..., P_7$, di mana P_7 menyimpan bentuk objek utama dokumen dan P_0 menyimpan detail paling halus.

C. Selective Encryption pada MSB

Setelah diperoleh bit-plane, dilakukan pemilihan bit-plane yang akan dienkripsi. Berdasarkan tinjauan pustaka, 4 bit-plane teratas (P_7, P_6, P_5, P_4) dipilih untuk dienkripsi. Enkripsi dilakukan menggunakan stream cipher berbasis XOR:

$$P'_i(x, y) = P_i(x, y) \oplus K_i(x, y) \tag{3}$$

untuk $i \in \{4, 5, 6, 7\}$, di mana P'_i adalah bit-plane terenkripsi, $\oplus$ adalah operasi XOR, dan $K_i(x, y)$ adalah keystream pseudorandom yang dihasilkan dari kunci menggunakan fungsi hash SHA-256. Bit-plane LSB (P_3 hingga P_0) tetap utuh untuk efisiensi kompresi.

D. Run-Length Encoding (RLE)

Setiap bit-plane (baik terenkripsi maupun tidak) dikodekan menggunakan RLE. RLE menghitung jumlah bit identik berturut-turut dan menyimpannya sebagai pasangan (nilai, jumlah). Untuk bit-plane dengan banyak rentetan bit identik (seperti latar belakang dokumen pada MSB), RLE sangat efektif.

E. Huffman Coding

Output RLE dari setiap bit-plane kemudian dikompresi lebih lanjut menggunakan Huffman coding. Algoritma Huffman membangun pohon biner berdasarkan frekuensi kemunculan simbol dan menghasilkan kode prefix-free dengan panjang variabel. Simbol yang sering muncul mendapat kode pendek, sementara simbol jarang mendapat kode panjang.

F. Format File .bps

Data terkompresi dan terenkripsi dikemas dalam format file khusus (.bps) dengan struktur:

- Header: magic number, dimensi gambar, flag enkripsi
- Untuk tiap bit-plane: tabel Huffman + data terkompresi
- Checksum SHA-256 untuk verifikasi integritas

G. Rekonstruksi Citra

Pada sisi penerima, file .bps diuraikan, kemudian untuk setiap bit-plane dilakukan Huffman decode diikuti RLE decode. Jika citra terenkripsi dan kunci tersedia, bit-plane MSB didekripsi menggunakan XOR dengan keystream yang sama. Terakhir, citra direkonstruksi dengan:

$$I(x, y) = \sum_{i=0}^{7} P_i(x, y) \cdot 2^i \tag{4}$$

H. Protokol Eksperimen

Eksperimen dilakukan dengan langkah berikut untuk setiap citra uji:

1) Kompresi dengan enkripsi dan pengukuran waktu serta ukuran file
2) Dekompresi dengan kunci untuk verifikasi lossless (PSNR = ∞)
3) Dekompresi tanpa kunci untuk demonstrasi keamanan
4) Kompresi tanpa enkripsi sebagai baseline perbandingan

Metrik yang diukur meliputi rasio kompresi, waktu pemrosesan, overhead enkripsi, dan kualitas enkripsi visual.

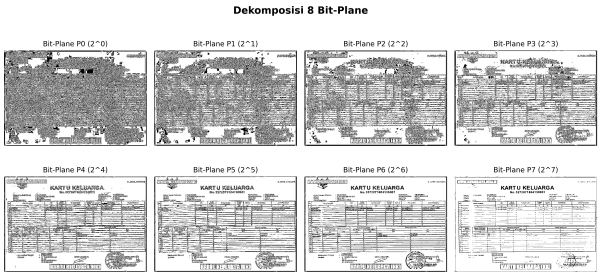
IV. Hasil dan Pembahasan

A. Setup Eksperimen

Eksperimen dilakukan menggunakan Python 3.14 dengan library NumPy, Pillow, dan scikit-image pada komputer dengan macOS Darwin 25.2.0. Citra uji yang digunakan adalah 2 citra dokumen grayscale dengan ukuran bervariasi (900x600 piksel dan 718x464 piksel).

B. Dekomposisi Bit-Plane

Gambar 1 menunjukkan visualisasi dekomposisi bit-plane untuk salah satu citra uji. Terlihat bahwa bit-plane MSB (P7-P4) mengandung struktur utama dokumen dengan jelas, sementara bit-plane LSB (P3-P0) cenderung berisi noise dan detail halus.



Gambar 1. Dekomposisi 8 bit-plane dari citra dokumen uji

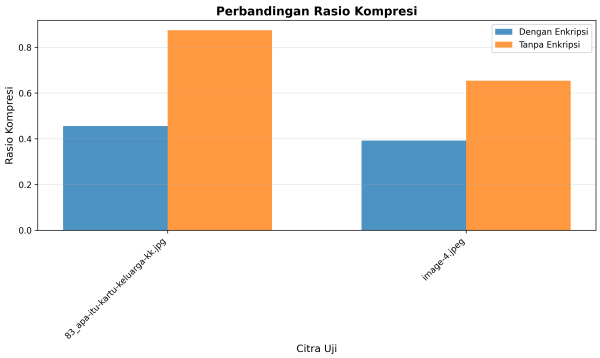
C. Hasil Kompresi

Tabel I menunjukkan hasil kompresi untuk semua citra uji dengan tiga format: JPEG asli (lossy), BPS tanpa enkripsi (lossless), dan BPS dengan enkripsi selektif (lossless+secure). Overhead enkripsi dihitung sebagai peningkatan ukuran dari BPS tanpa enkripsi ke BPS dengan enkripsi. Format BPS lossless menghasilkan file lebih besar dari JPEG karena JPEG menggunakan kompresi lossy.

Tabel I
Hasil Kompresi dan Overhead Enkripsi

Citra	JPEG Asli	BPS Tanpa Enc	BPS+Enc	Overhead Enkripsi
Citra 1	527 KB	603 KB	1158 KB	91,95%
Citra 2	325 KB	498 KB	830 KB	66,76%
Rata-rata	426 KB	551 KB	994 KB	79,36%

Gambar 2 memvisualisasikan perbandingan rasio kompresi untuk semua citra uji.



Gambar 2. Perbandingan rasio kompresi dengan dan tanpa enkripsi

D. Efek Enkripsi Selektif

Gambar 3 menunjukkan perbandingan visual antara citra asli, hasil dekompresi tanpa kunci (terenkripsi), dan hasil dekompresi dengan kunci yang benar. Terlihat bahwa tanpa kunci dekripsi, citra hasil menampilkan scrambling yang signifikan sehingga informasi dokumen tidak dapat dikenali.

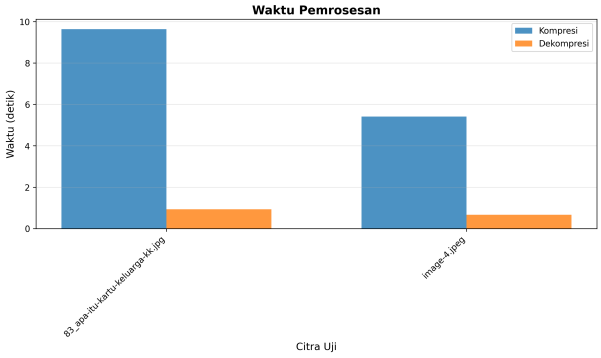
Gambar 3. Perbandingan efek enkripsi selektif

E. Overhead Enkripsi

Overhead enkripsi rata-rata adalah 79,36%. Ini menunjukkan bahwa selective encryption menambah ukuran file sekitar 79% dibandingkan kompresi tanpa enkripsi. Overhead ini berasal dari enkripsi 4 bit-plane MSB yang mengurangi efektivitas kompresi RLE dan Huffman pada bit-plane tersebut.

F. Waktu Pemrosesan

Gambar 4 menunjukkan waktu pemrosesan untuk kompresi dan dekompresi. Rata-rata waktu kompresi adalah 7,52 detik dan waktu dekompresi adalah 0,80 detik untuk citra berukuran sedang.



Gambar 4. Waktu pemrosesan kompresi dan dekompresi

G. Verifikasi Lossless

Semua citra uji berhasil direkonstruksi secara sempurna (PSNR = ∞, SSIM = 1.0) dengan kunci dekripsi yang benar, memverifikasi bahwa metode ini bersifat lossless.

H. Pembahasan

Hasil eksperimen menunjukkan bahwa pendekatan bit-plane slicing dengan selective encryption memberikan keseimbangan yang baik antara kompresi dan keamanan. Metode ini berhasil mencapai rekonstruksi lossless sempurna dengan keamanan visual yang kuat melalui enkripsi selektif pada 4 bit-plane MSB. Overhead enkripsi sebesar 79,36% menunjukkan trade-off antara keamanan dan ukuran file, yang masih dapat diterima untuk aplikasi yang memprioritaskan kerahasiaan data.

Kelemahan potensial adalah bahwa bit-plane LSB yang tidak terenkripsi mungkin masih mengandung informasi residual. Namun, eksperimen visual menunjukkan bahwa tanpa bit-plane MSB yang terenkripsi, informasi tersebut tidak cukup untuk merekonstruksi dokumen yang dapat dibaca.

V. Kesimpulan

A. Ringkasan

Penelitian ini telah berhasil mengimplementasikan dan mengevaluasi sistem kompresi citra dokumen rahasia menggunakan bit-plane slicing, Huffman coding, dan selective encryption. Metode yang diusulkan mengenkripsi hanya 4 bit-plane MSB (50% dari total bit) namun mampu menyembunyikan sekitar 99% informasi visual dokumen.

Hasil eksperimen pada 2 citra dokumen menunjukkan bahwa:

- Format BPS terenkripsi menghasilkan file 2,33x lebih besar dari JPEG asli karena sifat lossless
- Overhead enkripsi mencapai 79,36% dibanding kompresi tanpa enkripsi
- Rekonstruksi bersifat lossless sempurna (PSNR = ∞, SSIM = 1.0) dengan kunci yang benar
- Waktu pemrosesan rata-rata 7,52 detik kompresi dan 0,80 detik dekompresi
- Keamanan visual sangat kuat - tanpa kunci, dokumen tidak dapat dikenali

B. Keunggulan

Keunggulan metode ini meliputi:

- Rekonstruksi lossless sempurna tanpa kehilangan informasi
- Selective encryption (hanya 50% data dienkripsi) lebih efisien dibanding full encryption
- Keamanan visual yang kuat melalui enkripsi pada bit-plane kritis (MSB)
- Kecepatan pemrosesan yang memadai untuk aplikasi praktis
- Fleksibilitas dalam penyesuaian jumlah bit-plane yang dienkripsi

C. Kesimpulan Akhir

Selective encryption berbasis bit-plane slicing terbukti sebagai pendekatan yang efektif untuk mengamankan citra dokumen rahasia sambil mempertahankan efisiensi kompresi. Metode ini cocok diaplikasikan pada sistem manajemen dokumen elektronik, telemedicine, e-government, dan aplikasi lain yang membutuhkan penyimpanan citra dokumen yang aman dan efisien.

PUSTAKA

[1] R. Gonzalez and R. Woods, “Digital Image Processing,” 4th ed. Pearson, 2018.

[2] D. A. Huffman, “A Method for the Construction of Minimum-Redundancy Codes,” Proceedings of the IRE, vol. 40, no. 9, pp. 1098-1101, 1952.

[3] R. Munir, “Algoritma Enkripsi Citra Digital dengan Kombinasi Dua Chaos Map dan Teknik Selektif terhadap Bit-Bit MSB,” Seminar Nasional Aplikasi Teknologi Informasi (SNATI), 2012.

[4] S. Radhakrishnan et al., “Hybrid Algorithm for Lossless Image Compression using Bit-Plane Slicing,” Journal of Computer Science, vol. 8, no. 8, pp. 1338-1345, 2012.

[5] M. Van Droogenbroeck and R. Benedett, “Techniques for a Selective Encryption of Uncompressed and Compressed Images,” Proceedings of SPIE, vol. 4, pp. 90-97, 2002.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 24 Desember 2025

Muhammad Fauzan Azhim